UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW AND COMMERCIAL REGULATION

Volume 16 | Number 2 Article 8

Fall 1991

Transborder Data Flows and the Sources of Public International Law

Olga Estadella-Yuste

Transborder Data Flows and the Sources of Public International Law

Cover Page Footnote
International Law; Commercial Law; Law

Transborder Data Flows and the Sources of Public International Law

*Olga Estadella-Yuste**

OUTLINE:

* L.L.M. 1988, Columbia University School of Law; J.S.D. Candidate, Columbia University School of Law.

I. Introduction

The computer revolution and innovations in telecommunications greatly increased the ability to transfer information across national boundaries. With these two technological advancements, Transborder Data Flow (TDF) arose as a "new" issue in the international arena that needed to be identified and defined internationally.[1] The impacts of the new technologies of communication are world-wide; drawbacks and benefits are not limited to one country or individual. Accordingly, they affect the international community as a whole.

One definition of TDF is data and/or information transfer across national borders, usually in machine-readable form, and usually over telecommunication facilities.[2] In a narrower sense, TDF takes place through transnational computer-communication systems. Such arrangements are made through the connection of many computers in several countries. Events such as the expansion of world trade, and the internationalization of information-intensive industries like banking, insurance and tourism have intensified the need to ensure an instantaneous availability to disseminate data.[3]

---

[1] *See* Fishman, *Introduction to TDF*, 16 STAN. J. INT'L L. 1 (1980).

[2] The Centre on Transnational Corporations of the UN, which has carried out a thorough study on TDF, has defined TDF as the "movements, across national boundaries, of machine-readable data for processing, storage or retrieval." CENTRE ON TRANSNATIONAL CORPORATIONS, UNITED NATIONS, TRANSNATIONAL CORPORATIONS AND TRANSBORDER DATA FLOWS: A TECHNICAL PAPER, at 8, U.N. Doc. ST/CTC/23, U.N. Sales No. E.82.II.A.4 (1982) [Hereinafter Technical Paper].

There are some proposals aimed to change the term of TDF to international data services. According to one proposal, this term puts the focus on the services in their totality, rather than solely on the transfer—or flow—per se. *See* Robinson, *Legal Issues Raised by TDF*, 11 CANADA-U.S.L.J. 295 (1986).

[3] It has been calculated that booking reservations for a single Boeing 747 flight re-

The establishment of an international legal regime on TDF would affect the international community in various ways. First, the existence of a basic and uniform set of concepts and rules would facilitate and encourage the international exchange of information. Secondly, it would remove the fear that information sent abroad would be distorted which could consequently cause harm to the individual or interfere with the protection of privacy. Finally, a common approach to TDF would help to achieve the international cooperation promoted in the Charter of the United Nations.[4]

Although for some people this subject is still rather new, TDF has been a topic of discussion for more than 20 years. Many actions have been taken nationally and internationally during that time.[5] Since TDF appeared in the international context, rapid changes have occurred, necessitating a determination of what its international regulation should be. Now it is time to look back and determine whether the need for regulation of TDF has been met.

The purpose of this Article is to study what should be the international legal regime of TDF concerning personal data. Although the TDF issue can be approached by using different fields of law, this Article is framed around Public International Law (PIL). In particular it concentrates on the roles that traditional sources of PIL have played in regard to TDF.

Part I of this Article examines the general approach to TDF. An historical background is followed by an analysis of how TDF has become an international concern. Part II focuses entirely on the role of the sources of public international law regarding TDF. According to article 38 of the Statute of the International Court of Justice, there are three sources of PIL: international conventions, customary international law, and the general principles of international law.

The analysis in Part I begins with an overview of the existing international legal instruments on TDF. This analysis shows that both the variety of competing interests involved and the different areas of law concerned have made it difficult to define and further develop an international legal regime on TDF. However, the work done by some international organizations has resulted, in some cases, in the adoption of legal instruments on very specific aspects of TDF. Although there is not a complete lack of regulation of TDF (particularly concerning personal data protection and within the Eu-

---

quires the transmission of 27,000 messages. B.W. Napier, Contractual Solutions to the Problem of Equivalent Data Protection in Transborder Data Flows 5 (March 28, 1990) (Paper presented at a conference on "Access to Public Sector Information, Data Protection and Computer Crime" held in Luxembourg, March 27-28, 1990).

[4] One purpose of the United Nations is "[t]o achieve international cooperation in solving international problems of an economic, social, cultural, or humanitarian character." U.N. CHARTER, art. 1.

[5] *See infra* notes 56, 17, and 11.

ropean context), the existing legal regime is far from complete; there is still a need to study the manner in which other sources of international law have contributed to the legal regulation of TDF.

Part II of this Article begins by examining whether an international custom or a regional custom exists concerning TDF. To this end, it must be determined what state practice has been by analyzing national laws on data protection, as well as analyzing the activities carried out by the national institutions that implement the data protection acts. On the other hand, whether and how the states have expressed their opinio juris on the TDF involving transfer of personal data and/or non-personal data must also be determined. The importance of examining whether there is any customary law not only stems from the general advantages derived from the recognition of customary law,[6] but also from the fact that its existence would provide uniformity and unity to the issue of TDF. If such custom turns out to be only regional, then its adoption may extend to the rest of the international community.

Part II of this Article next addresses how some of the existing general principles of international law may apply to TDF. First of all, a new approach to the two traditional principles that have been linked to TDF is needed. These two principles are freedom of information and national sovereignty. Broadly defined, the first principle seems to prohibit any barriers to the transmission of information. The principle of national sovereignty grants power to the states to establish rules regulating the flow of information. These two principles are sometimes wrongly linked to TDF. Therefore, it is obvious that these two definitions need to be balanced in order to make them compatible for application to TDF.

Finally, this Article attempts to integrate other general principles of international law that are "recognized by civilized nations" from some of the international data protection instruments and to apply them to TDF.

II. Approach to Transborder Data Flows

A. Historical Background

1. International Level

The international conference on Human Rights held in Tehran in 1968 by the UN, on the twentieth anniversary of the Universal Declaration of Human Rights, paved the way to the "data revolution."[7] One of the fundamental issues addressed by this conference

---

[6] *See generally* Meron, *The Geneva Conventions as Customary Law*, 81 AM. J. INT'L L. 348 (1987).

[7] F. HONDIUS, EMERGING DATA PROTECTION IN EUROPE (1975). *See* Hondius, *Data Law in Europe*, 16 STAN. J. INT'L L. 87, 90 (1980).

was the use of "electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society."[8]

Not all of the participating countries had a similar response to the issue. At that time, third world countries did not consider the use of data to be a real problem. Rather, their concern was focused on the access to the technology needed to process data or transfer technology. The Western world adopted a twofold approach carried out in different manners by the Organization for Economic Cooperation and Development (OECD) and the Council of Europe; each of these organizations dealt with the issue in accordance with their own goals.

The OECD approached two important ideas: (i) the impact of computers and telecommunication technology influencing the sending of information; and (ii) the regard of information as a commodity traded nationally and internationally.[9] In addition, individual member states stressed the fact that such "information power"[10] would have important social and economic consequences, and that some rights should be established to protect the parties to whom the information relates.

Among the most important initiatives taken by the OECD were the promulgation of Guidelines governing the protection of privacy and TDF of personal data,[11] and a Declaration on TDF.[12] The Guidelines were drafted with the purpose of reaching an international harmonization of principles and guaranteeing minimum standards of personal privacy.[13] The Declaration stressed the economic

---

[8] This issue was reflected in a United Nations Resolution. G. A. Res. 2450, 23 U.N. GAOR Supp. (No. 18) at 54, U.N. Doc. A/7218 (1968).

[9] Since 1974, the OECD has had working groups of TDF policy analysts; these working groups continue to operate today. The OECD has organized many symposiums and conferences in which an important number of its member states have participated with papers and presentations. *See, e.g.*, ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, INFORMATION COMPUTER COMMUNICATIONS POLICY No. 1, TRANSBORDER DATA FLOWS AND THE PROTECTION OF PRIVACY (1979); Department of Communication, Canadian Government, *Policy Implications of TDF, reprinted in* OECD Directorate for Science, Technology and Industry (1980) (DSTI/ICCP/80.20).

[10] As it was first pointed out, "information is power, and economic information is economic power." Speech given by Louis Joinet, French Minister of Justice, at the OECD Symposium on Transnational Data Flows and Protection of Privacy Impacts and Trends, Vienna, Austria (Sept. 20-23, 1977).

[11] ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1981) [hereinafter Guidelines]. These guidelines were eventually endorsed by 22 members.

[12] OECD, *Declaration on Transborder Data Flows*, ACTIVITIES OF OECD IN 1985, at 88-89 (1986) [hereinafter Declaration].

[13] Such a mandate was given to the OECD Working Party on Transborder Data Flows of the Committee on Computer, Information and Communications Policy. Grewlich, *Controlling International Information Economy Conflicts*, TRANSNAT'L DATA AND COMM. REP., Sept. 1989, at 13, 14 [hereinafter TDR]. The mandate directed the committee "to concentrate its work primarily on the economic, legal and social policy issues raised by transborder data flows. In particular, it is required to examine the extent and impact of these flows,

issues, rather than the technical ones, raised by the internationalization of modern telecommunication, data processing, and information services.[14]

In its approach to TDF, the Council of Europe stressed the relationship between technology and human rights.[15] Its main concern was privacy protection and the mechanisms that could be used nationally and internationally to protect personal data.[16]

In 1981, after a period of study, the Council of Europe adopted a Convention on the "Protection of Individuals with Regard to Automatic Processing of Personal Data".[17] The Convention established certain requirements for the storage, collection, and processing of personal data, as well as specific provisions on TDF.[18] Since then, however, the Committee of Experts selected by the Committee of Ministers has not only adopted other sectorial recommendations applied to specific sectors, but also has studied the impact of new technologies in other fields of interest, such as telemetry and electronic mail.[19]

At the same time, international organizations were created to deal with issues concerning TDF and data protection. Thus, the Intergovernmental Bureau for Informatics (IBI) was created mostly by developing countries that lacked explicit policies and regulatory frameworks on informatics and TDF. Although the IBI adopted a series of recommendations concerning TDF, the dissolution of the

---

analyze the principal factors underlying their growth, identify the major government policies which have an impact on these flows, ascertain what legal or other measures might be required to deal with these issues and recommend areas for international cooperation." *Id.*

[14] *See* Declaration, *supra* note 12.

[15] The Council's Parliamentary Assembly recommended that the Committee of Ministers study the possible dangers on human rights posed by the use of modern scientific and technical equipment. *Recommendations of the Parliamentary Assembly*, Eur. Consult. Ass., 19th. Sess., Doc. No. 509 (Feb. 1968).

[16] The European Convention on Human Rights states that "everyone has the right to respect for his private life." European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, art. 8. The Parliamentary Assembly was particularly concerned whether this article was enough to protect the right of privacy in view of the developments in information processing. The Committee of Ministers concluded that a positive action to protect the right to privacy was necessary.

[17] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Europ. T.S. No. 108, 20 I.L.M. 317 (1981) [hereinafter Convention]. The Convention came into force on October 1, 1985, after five countries had ratified—Sweden, France, Norway, Spain and Germany. Since then, Austria, Belgium, Cyprus, Denmark, Greece, Iceland, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Turkey and the United Kingdom have signed the Convention. Only Austria, Denmark, Luxembourg, Ireland, and the United Kingdom have ratified it, and further ratifications are expected this year. For a detailed study on the negotiations and further analysis of the Convention, see Garzon Clariana, *La Protección de los Datos Personales y la Función Normativa del Consejo de Europa*, 8 REVISTA DE INSTITUCIONES EUROPEAS 9 (1981).

[18] *See* Convention, *supra* note 17.

[19] COUNCIL OF EUROPE, NEW TECHNOLOGIES: A CHALLENGE TO PRIVACY PROTECTION? (1989).

IBI in 1987 has caused the recommendations to lose the international relevance once achieved.[20] For this reason, this Article does not address its work in depth, with the exception of a few specific points.[21]

The United Nations has also undertaken some work on issues related to TDF. The Center on Transnational Corporations has carried out a series of studies on TDF and its relevance to multinational corporations.[22] Furthermore, the Commission of Human Rights has recently revised a draft of Guidelines concerning "Computerized Personal Data Files," has been brought as a result of the Economic and Social Council before the General Assembly for final adoption at its forty-fifth session.[23] The principles stated in the draft of the Guidelines are purported to be the minimum guarantees to be implemented into national legislation.[24] Since those principles come very close to those of the OECD Guidelines and COE Convention this Article does not include a separate study of them; however, a brief analysis and some comments are made.

2. *National Level*

Discussions concerning TDF were not limited to the international level. State representatives and national experts also began to consider the problems involved in the transfer of data, and how these problems could affect their respective countries. It became

---

[20] Some commentators have pointed out that the lack of effectiveness of the IBI was due not only to the problems in coordinating its work, but also to the actions of corporations and states to block the development of policies incorporating "state" information rights. *See* McDowell, *The Shaping of TDF Policy*, TDR, May 1989, at 19, 21.

[21] *See infra* note 245 and accompanying text.

[22] Among those studies are: Technical Paper, *supra* note 2; TDF: TNCs AND REMOTE SENSING DATA, U.N. Doc. ST/CTC/51, U.N. Sales No. E.84.II.A.11 (1984) [hereinafter REMOTE SENSING DATA STUDY]; TDF: ACCESS TO THE INTERNATIONAL ON-LINE DATA-BASE MARKET, U.N. Doc. ST/CTC/41, U.N. Sales No. E.83.II.A.1 (1982) [hereinafter ON-LINE DATA-BASE STUDY].

[23] The Sub-Commission on Prevention of Discrimination and Protection of Minorities drafted Guidelines on the use of computerized personal files. Res. 1988/29, U.N. Doc. E/CN.4/1989/3 - E/CN.4/Sub. 2/1988/45, Chap. II, § A (1988). The Commission on Human Rights recommended the Guidelines draft to the Economic and Social Council for its adoption. Res. 1989/43, U.N. Doc. E/1989/20, E/CN.4/1989/86 at 112 (1989). The Economic and Social Council decided to transmit to the General Assembly the final report for its adoption and publication. E.S.C. Res. 78, 1989 U.N. ESCOR Supp. (No. 1) at 62, U.N. Doc. A/44/49 (1989). The Resolution adopted by the General Assembly requests the Commission on Human Rights to examine and modify, if necessary, the draft guidelines. G.A. Res. 132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989). Finally, the revised version of the Guidelines was recommended, again, to the General Assembly for its adoption and publication through the Economic and Social Council (Draft Res. V, 1990). The guidelines were adopted during the 45th session. U.N. Doc. A/Res/45/95 (1991).

For the first version of the Guidelines concerning the regulation of computerized personal data files, see E/CN.4/Sub.2/1988/22 adopted on 21 July 1988. For the final version of the Guidelines, see E/CN.4/1990/72 [hereinafter UN Guidelines].

[24] *Id.*

clear that the location of data bases in a country which lacked a data protection law guaranteed the free flow of information across boundaries.[25]

To a certain extent, the practice adopted by the states has been different. During the drafting process of the first national laws on data protection, the discussion focused on two issues—the sending of personal data across boundaries and the protection of the individual. As a result, the countries that have enacted laws on data protection have covered personal data exclusively, rather than personal data along with commercial data or business information. However, some of these national laws cover the personal data held by legal persons.[26] The reason why most of the countries did not include legal persons within the scope of protection was because of the strong opposition of the business community and their criticism of such regulation.[27]

It is important to point out that since the debate on TDF arose, there has been a shift in its focus. The debate started with privacy protection and personal data protection, then moved to "protectionist paranoia,"[28] and finally, to a trade in services.[29] Many reasons have been suggested to explain this shift. It has been said that the beginning of the debate on TDF involved too many experts, therefore making it difficult to achieve consensus. This coalition was able to move the discussion to trade terms, which restricted the participation of the expert community and postponed some of the international debate, such as free flow of information versus restriction.[30]

B. Transborder Data Flow—An Issue of International Concern

1. General Approach

TDF has an important impact in international relations as a re-

---

[25] Those countries without data protection laws are categorized as "data havens." Some scholars state that data haven countries are not necessarily using this status to pursue international business because their own information can be disseminated without their knowledge or permission. *See* Hondius, *supra* note 7, at 103.

[26] Austria, Denmark, Iceland, Luxembourg, and Norway include legal persons within the provisions of their data protection acts. *See infra* note 79. France's data protection laws' right of access was extended to legal persons on July 3, 1984 by an administrative decision of the National Commission on Informatics and Liberties data protection authority. *See id.* and accompanying text.

[27] Their argument was that such regulation would have very negative consequences in their business because it would be like a protectionist barrier. *See infra* note 141.

[28] Robinson, *TDF Issues: Hard Choices for Governments*, TELECOMMUNICATIONS POL'Y, Dec. 1989, at 5.

[29] *See generally* Sauvant, *The Role of Transborder Data Flows in the International Services Debate*, 8 DEV. AND PEACE 113 (1987).

[30] McDowell states that the role policy research programs played in managing the relations among dominant states in international organizations closed off the transborder question. McDowell, *supra* note 20, at 22. In his discussion, he wonders whether these organizational research programs adequately represent all interests, both international and national. *Id.*

sult of its increased use by the international community.[31] The storage and the process of any kind of data is done internationally on a regular basis for a variety of reasons, such as for a lack of appropriate computer equipment, or for a lack of highly qualified experts.

During the past 20 years, TDF has raised more problems of international concern than solutions that have been provided. TDF can be characterized as a multifaceted phenomenon that raises issues in different areas of law. Although this Article neither studies them all nor gives a simplistic approach to TDF, it is necessary to point out some of those areas. Among the different areas of law that relate to TDF are conflicts of law, public international law, computer crime, intellectual property, corporate law, and tax law.[32]

Two levels of influence on TDF have been identified that are relevant to public international law. These two levels are a "macro" and a "micro" level.[33] The first category deals with the concern for national sovereignty and cultural identity resulting from the information transfer.[34] The micro level focuses on the individual and his access to and the protection of "his" data held in a foreign jurisdiction.[35] The identification of these two levels does not exclude the possibility that some issues may be included in both categories at the same time (e.g., information about a country's mineral resources may be both governmental and personal). It is even possible to identify an intermediate level that would include business aspects identifiable neither at the state level nor at the individual level.

Not all states have given the same relevance and solutions to each of the three levels identified. For instance, Canada has been traditionally concerned about the protection of its national sovereignty,[36] Sweden about the vulnerability of its society in general,[37]

---

[31] TDF can involve the transmission of either personal data or non-personal data. For example, France refused to transfer data stored in France concerning prisoners of the Spanish civil war because there is no data protection law in Spain. *Commissioners Stress TDF Risks*, TDR, Nov. 1989, at 5, 6. The importation of information processing services into Canada resulted in lost revenues of $150 million to $300 million in 1976, and may have cost Canadians 30,000 to 40,000 jobs, either because they were lost or were never created. *Canadian TDF Job Losses Reported*, TDR, Aug. 1984, at 439; Pipe, *Are Canadian Jobs Lost Through TDF?*, TDR, Mar. 1985, at 132.

[32] For a general approach to the different issues related to TDF, see Gotlieb, Delfan & Katz, *The Transborder Transfer of Information by Communications and Computer System: Issues and Approaches to Guiding Principles*, 68 AM. J. INT'L L. 227 (1974); M. KIRBY, LEGAL ASPECTS OF INFORMATION TECHNOLOGY 10 (OECD Series of Information Computer Communication Policy No. 8, 1983); Robinson, *supra* note 2, at 297.

[33] Gotlieb, *Impact of Technology on Contemporary International Law*, 170 RECEUIL DES COURS 119, 128 (1981).

[34] *Id.*

[35] *Id.*

[36] Robinson, *Sovereignty and Data: Some Perspectives*, in THE INFORMATION ECONOMY: ITS IMPLICATIONS FOR CANADA'S INDUSTRIAL STRATEGY, PROCEEDINGS OF A CONFERENCE HELD AT ERINDALE COLLEGE, UNIVERSITY OF TORONTO MAY 30 - JUNE 1, 1984 330 (1984).

[37] SWEDISH MINISTRY OF DEFENSE, THE VULNERABILITY OF THE COMPUTERIZED SOCIETY (1978).

other European countries about protecting their private corporations, while the USA has been promoting a free flow of information[38] and developing countries have pointed out problems related to the location of economic activities and the invasion of their national culture.[39]

To study these three levels with great detail would require an extremely long paper. Thus, this Article focuses on the micro level, however, some references are also made to the intermediate level.

2. *Specific Points of Discussion of TDF*

TDF has raised very interesting debates about its own terminology. Due to the length of the different doctrinal positions, the main points of these arguments are briefly summarized below.

One of the traditional issues of discussion is whether information and data are synonyms. The interesting part of this debate is that each approach raises some complementary issues of discussion that involve other areas of law, such as remote sensing data.[40]

Another issue is whether information should be qualified as a service or as a commodity. The significance of this debate is that its answer determines the nature of the applicable rules. Legal duties and obligations will differ if information is considered a commodity rather than a service. For example, if one qualifies information as a commodity, it can be the object of expropriation; otherwise, it could not be expropriated.[41]

A third issue of discussion is whether property rights can be extended to information. Many scholars are divided because, although

---

[38] Hondius, *supra* note 7, at 90. Cole, *New Challenges to the US MNCs in the European Economic Community: Data Protection Laws*, 17 N.Y.U. INT'L L. & POL'Y 893 (1985).

[39] Sauvant, *TDF and the Developing Countries*, 37 INT'L. ORG. 360 (1983). Allotey, *Consideraciones Sobre FDI en los Paises en Desarrollo*, 3 AGORA 40 (1984). Ennison, *Legal Aspects of TDF in Developing Countries: Sovereignty Considerations*, 12 INT'L BUS. LAW. 163, 164 (1984).

[40] The data collected through remote sensing satellite need to be processed before they can be read and used as an information source. Some scholars have supported the idea that data constitute the raw material for information, and that data are the basic resource from which information is produced. *See* Groshan, *TDF: Is the Idea of an International Regime Relevant in Establishing Multilateral Controls and Legal Norms?*, 14 LAW/TECH. 1 (1981). *See generally Remote Sensing Data Study*, *supra* note 22.

Other scholars argue that there is no difference between information and data except for the time at which they were created. "Data" belongs to the computer era and "information" to the "pre-computer" era. *See* Garzon Clariana, *El Marco Juridico del Flujo de Dotos Iransfranteros*, IBI, TDF 206 (1984).

I agree with this last position. Creating two different notions merely confuses both concepts. Bearing this in mind, I shall use these terms interchangeably throughout this Article.

[41] Studies on the expropriation of information have been made. *See* Horgan, *Foreign Data: Is it Safe in US Data Banks?*, 16 CALIF. WEST. INT'L L.J. 347 (1986). Some other scholars have noted that information has a dual connotation as a service and as a commodity. Pierre Catala has reached the conclusion that the best way to identify information is as an object, as an informing fact. Catala, *Cinco Preguntas a Pierre Cotolo*, 2 AGORA 39 (1983). His conclusion reconciles to a certain degree both concepts: service and commodity. *Id.*

information is not a tangible good, it can be stolen or diverted. In some countries, this question has even reached the highest court.[42]

TDF involves not only a variety of issues and competing interests, but also the participation of different actors. Information activities are performed by sovereign states, and by non-state actors, such as multinational corporations, transnational organizations, communication carriers, and other private organizations.[43]

Not all of these actors are subjects of public international law. Some of them, however, have become in recent years a source of controversy due to their economic and even political power in the international arena. This is especially true for multinational corporations (MNCs). Only subjects of public international law participate in the creation of its norms and are internationally responsible for their actions. However, some people argue that MNCs have participated in the international legal system.[44] The discussion on TDF provides once more an opportunity to stress the necessity of bringing private corporations, to a certain extent, under the wings of public international law because of the relevant role they play in sending, storing, and processing information throughout the world.[45]

The nature of the data used can be personal or non-personal. Within the international business framework, both types of data are used in daily activities; however, the transborder flow of non-personal data is much higher than that of personal data. According to some studies, most of the information transferred relates to international business, and only ten percent of the information refers exclusively to personal data.[46] These numbers may seem shocking, particularly if one recalls that when the problem first arose, the international community's major concern was for the protection of personal data. In any event, the low percentage of personal information transferred does not mean that the international concern was unjustified.

The nature of information sent abroad becomes important when determining the rules to be applied to TDF. For example, personal and business data—or non-personal data—may need different time

---

[42] The Canadian Supreme Court has ruled that some information, such as confidential or business information, could be regarded as property and hence be entitled to the protection of the criminal law. R. v. Stewart, 1 R.C.S. 963, 964 (1988). For a broad discussion of the issue, see Weinrib, *Information and Property*, 38 U. TORONTO L.J. 117 (1988); Hammond, *Theft of Information*, 100 L.Q. REV. 252 (1984); and Branscomb, *Who Owns Information?*, TDR, June 1986, at 9.

[43] *See generally* ON LINE DATA-BASE STUDY, *supra* note 22.

[44] Charney, *Transnational Corporations and Developing Public International Law*, 1983 DUKE L.J. 748, 762.

[45] To study what role the transnational corporations have played on TDF, see Technical Paper, *supra* note 2; ON-LINE DATA-BASE STUDY, *supra* note 22, and REMOTE SENSING DATA STUDY, *supra* note 22.

[46] Rankin, *Business Secrets Across International Borders: One Aspect of the TDF Debate*, 10 CANADIAN BUS. L.J. 221 (1985).

limitations for its storage and updating and may need different requirements for its protection. Moreover, the consent required from an individual to whom the information refers may be taken into consideration in different ways depending on whether the data transferred is private or not.

In relation to the above section on the nature of data used, this Article uses the following classifications of the types of activities that lead to the creation of TDF. These classifications combine the different participants using TDF and the nature of the information they use. Thus, these activities can be classified as follows:[47]

Intra-corporate information transfer. This usually involves an exchange of internal administrative information, customer service, or a maintenance of records.[48]

International information transfer. This occurs when national governments cooperate in administrative or security matters.[49]

Transnational pursuit of information resources. This activity involves the private sector when: a) data processing can be performed more cheaply abroad; b) vital information is only available abroad; or c) circumvention of national laws is sought.

TDF has been an issue on the international agenda in the last twenty years as a result of the different areas of law involved, the variety of compelling interests, the actors participating, and the different activities that create TDF. While conventions and guidelines are being drafted to lay down the international relations involved in data protection, and in particular TDF, it may be necessary to examine whether there are any other sources of international law that are regulating this new area of law. Undoubtedly, the first steps taken by the OECD and the Council of Europe constitute an important basis for approaching TDF as an issue of international concern. However, there is still much more to be done.

---

[47] Yarn, DEVELOPMENT OF CANADIAN LAW ON TRANSBORDER DATA FLOW, 13 GA. J. INT'L & COMP. L. 825, 827 n. 8 (1983).

[48] About 80-90% of the trade in data services consists of non-commercial or intra-firm transactions. K. SAUVANT, INTERNATIONAL TRANSACTIONS IN SERVICES: THE POLITICS OF TDF 7 (1986). The Canadian Department of Communication has estimated that such activities constitute 90% of the flows between the subsidiaries and headquarters of multinational organizations. Rankin, *supra* note 46, at 221.

[49] For instance, Canada and the United States regularly exchange information on defense, taxation and criminal activities. Yarn, *supra* note 47, at 827. Moreover, France, Germany, Belgium, The Netherlands and Luxembourg concluded an agreement in Schengen (Luxembourg) which provides for the establishment of the Schengen Information System (SIS), a system for the exchange of computerized data. Fauvet, *Privacy in the New Europe*, TDR, Nov. 1989, at 17, 18. The SIS is confronted with problems related to the diversity of existing legislation: Belgium has no legislation, the Dutch legislation excludes police files and Spain, which has no legislation, is seeking to become a party to the Agreement. *Id.* The agreement was signed on June 14, 1985, and became fully effective on March 2, 1986. *Id. See* H. MEIJERS, INTERNATIONALISM OF CENTRAI CHAPTERS OF THE LAW ON ALIENS, REFUGEES, PRIVACY, SECURITY AND THE POLICE (1991).

III. Role of the Sources of Public International Law Regarding Transborder Data Flows

A. Overview of the Existing Legal Instruments

As mentioned at the beginning of this Article, the main existing legal instruments that regulate some aspects of TDF are the "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data"[50] adopted by the Council of Europe, the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"[51] and the "Declaration on TDF,"[52] both adopted by the OECD. A comparative study shall be pursued on the main provisions of those instruments—first, the COE Convention and the OECD Guidelines.

Even though the nature of the COE and OECD is different, the instruments on TDF adopted by these two organizations have important similarities. Not only is their structure fairly similar,[53] but also some of their substantive provisions are similar. For example, the OECD Guidelines and the COE Convention do not merely recognize a right to privacy; instead, they both recognize the need to reconcile the fundamental values of respect for privacy and the free flow of information between people.[54] Furthermore, the provisions on TDF included in both instruments are related to the transmission of personal data, rather than that of non-personal data.

With respect to the UN Guidelines, it is important to add that although they contain a reference to the protection of privacy.[55] These Guidelines basically consist of an enumeration of principles stating the minimum guarantees computerized personal files and on providing some regulations on TDF.

---

[50] *See* Convention, *supra* note 17.

[51] Guidelines, *supra* note 11.

[52] Declaration, *supra* note 12.

[53] On the one hand, the convention is divided into the following chapters: chapter I - General provisions; chapter II - Basic principles for data protection; chapter III - Transborder data flows; chapter IV - Mutual assistance; chapter V - Consultative committee; chapter VI - Amendments; chapter VII - Final clauses. Convention, *supra* note 17. On the other hand, the Guidelines has the following sections: § 1 - General part; § 2 - Basic principles of national application; § 3 - Basic principles of international application: free flow and legitimate restrictions; § 4 - National implementation; § 5 - International co-operation. Guidelines, *supra* note 11.

[54] The Convention "recogniz[es] that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples." *See* Convention, *supra* note 17. The Recommendation of the Guidelines recognizes that "[m]ember countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information." Guidelines, *supra* note 11, at 7.

[55] The only reference to the protection of privacy is made in the TDF clause in the following terms: "When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned." *See* U.N. Guidelines, *supra* note 23.

Secondly, this Article addresses the OECD Declaration. Its importance rests in the fact that it was the first multilateral instrument to deal with TDF of non-personal data.

1. The Convention and Guidelines on TDF

It is important to remember that at the time the COE Convention and the OECD Guidelines were adopted, TDF was a relatively new phenomenon, and most countries were not aware of either the problems involved or the need to enact national regulations. Thus, these instruments provided guidance and help to some state parties on how to regulate those areas of TDF involving the transmission of personal data. In contrast, countries that had existing laws were able to consider the possibility of adjusting their own laws to the provisions established in the COE Convention and OECD Guidelines.[56]

a. Legal Nature of the COE Convention and OECD Guidelines

The legal nature of these two instruments is one of the first distinctions necessary to address. The binding nature of the COE Convention was evident following its inception on October 1, 1985.[57] However, the moral force, or the non-binding nature of the Guidelines, has been a traditional topic of debate.[58] It is important to rec-

---

[56] Among the countries that first adopted data protection laws were: Austria with its Federal Act of 18 October 1978, on the Protection of Personal Data, §§ 25-27, Bundesgesetzblatt No. 565/1968 (Aus.); Denmark with its Public Authorities' Registers Act, No. 294 (1978) (Den.), *reprinted in* Expert Group on Transborder Data Barriers and the Protection of Privacy, Working Party on Information, Computer and Communications Policy, OECD Directorate for Science, Technology and Industry, Compilation of Privacy Legislation in OECD Member Countries (Mar. 5, 1979) (DSTI/ICCP/79.11/05) [hereinafter OECD COMPILATION], Private Registers Act, No. 293 (1978) (Den.), *reprinted in* OECD COMPILATION (DSTI/ICCP/79.11/05); France with its Act 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (1978) Journal Officiel de la Republique [J.O.] 227 F (Fr.), *reprinted in* OECD COMPILATION (DSTI/ICCP/79.11/08); Norway with its Act of 9 June 1978 Relating to Personal Data Registers, *reprinted in* OECD COMPILATION (DSTI/ICCP/79.11/14); Sweden with its Data Act of 11 May 1973, *reprinted in* OECD COMPILATION (DSTI/ICCP/79.11/18); Germany with its Federal Data Protection Act, (1977) BGB1 I 201, *reprinted in* OECD COMPILATION (DSTI/ICCP/79.11/01); United States with its Privacy Act of 1974, 5 U.S.C. § 552a (1976) (This Act covers only the Federal government).

For a general discussion on data protection laws, see Evans, *European Data Protection Law* 29 AM. J. COMP. L. 571 (1981); Hondius, *supra* note 7.

[57] Before its entry into force, the question was whether the signature obligates the signatory to avoid defeating the object and purpose of the treaty. *See* article 18 Vienna Convention on the Law of Treaties, UN, Doc. A/Conf. 39/27. *See generally*, Rogoff, *International Legal Obligations of Signatories to an Unratified Treaty*, 32 ME. L. REV. 263 (1980). One of the conditions established in the Convention was the need for its ratification by five countries before it comes into force. *Id.* at art. 22.2. For the signatures and ratification on the Convention, see Convention, *supra* note 17.

[58] In reference to the OECD Guidelines on Multinational Corporations, it has been said that "[t]he Guidelines are however *morally* binding. Their observance is sanctioned by public opinion and by the action governments may undertake." R. BLANPAIN, THE BADGER

ognize that the Guidelines do not have a well-identified legal nature.[59]

In any event, the fact that the Guidelines are neither legally binding nor a source of international law per se[60] does not preclude the possibility that they have legal implications.[61] Moreover, some governments have encouraged the voluntary endorsement by private corporations of the OECD Guidelines.[62]

b. Scope and Purpose of Both International Instruments

The COE Convention and the OECD Guidelines use similar terms to set up and recommend that member states adopt certain principles that should be observed in the transmission of information across national boundaries.[63] Likewise, both instruments call for mutual assistance and international cooperation towards the de-

---

CASE AND THE OECD GUIDELINES FOR MULTINATIONAL ENTERPRISES 38 (1977) (emphasis in the original).

See generally, Baade, *The Legal effects of Codes of Conduct for Multinational Enterprises* in LEGAL PROBLEMS OF CODES OF CONDUCT FOR MULTINATIONAL ENTERPRISES 3 (1980). Patrick, *Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and OECD Guidelines*, 21 JURIMETRICS J. 405 (1981).

[59] The comparison between the nature of the OECD Guidelines on Multinational Corporations (MNC) and the Guidelines on TDF is dangerous and they have to be differentiated. The Guidelines on MNC forms part of a Declaration while the Guidelines on TDF forms part of a Recommendation. The Convention which creates the OECD provides that Recommendations and Declarations have a different legal nature. The Recommendation which the Council may make to member states have a non-binding nature in contrast with the decisions or declarations. The "Declaration" is not included within the decisional process of the organization. It is a form which has been developed through practice and its effect is the same as the Decisions of the Council of the OECD. For further explanation of the different forms of decisions which are taken by the OECD, see Vogelaar, *The OECD Guidelines: their Philosophy, History, Negotiation, Form, Legal Nature, Follow up Procedures and Overview* in LEGAL PROBLEMS OF CODES OF CONDUCT FOR MULTINATIONAL ENTERPRISES 132-35 (1980).

[60] In relation to the OECD Guidelines on MNCs, Vogelaar has affirmed that "[t]he Guidelines therefore constitute a source of law that means a method to detect and determine rules of law as a positive factor in the process of law creation. Their role in preventing or resolving conflicts is to indicate, in the absence of express rules decisive on particular cases, how to find an equitable solution". *Id.* at 135.

[61] For a detailed study on non-binding international agreements, see Editorial Comment, *The Twilight Existence of Non-binding International Agreements*, 71 AM. J. INT'L L. 296 (1977). Professor Garzon Clariana has said that "a vote [for a] non-binding international text will possibly result followed by performance, in legitimate expectations on the part of other States. Obviously, in these and other cases much will depend on an appreciation in good faith of the circumstances." Garzon Clariana, *The Legal Significance of Data Protection for Regulation of Transborder Information*, in WORLD TELECOMMUNICATION FORUM: LEGAL SYMPOSIUM ON INTERNATIONAL INFORMATION NETWORKS I.4.1, I.4.2 (Geneva Symposium, 1983).

[62] "[T]he federal government is undertaking a programme to encourage private sector corporations to develop and implement voluntarily privacy protection codes." COMMUNICATIONS AND PUBLIC AFFAIRS, CANADA DEP'T OF JUSTICE, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TDF OF PERSONAL DATA: IMPLICATIONS FOR CANADA (1985). *See generally* Poullet, *Privacy Protection and TDF: Recent Legal Issues*, in ADVANCED TOPICS OF LAW AND INFORMATION TECHNOLOGY 35 (1989).

[63] Convention, *supra* note 17j Guidelines, *supra* note 11.

velopment of principles—both domestic and international—to govern the applicable law on TDF.[64] Moreover, these instruments recognize that the free flow of personal data is essential for transborder economic activities and that it is necessary to limit state interference with free flow of commercial data in the name of privacy protection.[65] However, neither the COE Convention nor the OECD Guidelines contain provisions on economic data; instead they narrow their scope to personal data.[66]

This sectional approach used by both instruments can be criticized. As stated earlier, the amount of personal data processed is very small when compared with that of economic data. Thus, it would be more important to have a convention or other multilateral instrument regulating economic or commercial data rather than personal data. However, it is obvious that the international community is not ready for such an enterprise, especially given the business sector's strong opposition.[67]

The purpose of the COE Convention is to secure respect for the individual rights and fundamental freedoms of every individual in the territory of each party, regardless of his nationality or residence, and in particular, his right to privacy concerning the automatic processing of personal data relating to him.[68] However, the objective of the OECD Guidelines is to recommend to member countries to take into account in their national legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines. In light of this objective, the OECD Guidelines recommend the removal of any unjustified obstacles to TDF.[69]

The scope of the COE Convention is limited to automated personal data files and automatic processing of personal data in the public and private sectors. In contrast, the OECD Guidelines' scope encompasses personal data that is processed, or that, due to its nature, may be used and therefore poses a danger to individual privacy.[70] In addition, the OECD Guidelines apply to both the public and the private sectors.[71]

Initially, the Convention was restricted to the protection of data held by physical persons, but it permits its extension to legal persons. This issue was considered problematic when determining the scope of the Convention, because it was not very clear whether the

---

64 Convention, *supra* note 17; Guidelines, *supra* note 11.

65 Convention, *supra* note 17; Guidelines, *supra* note 11.

66 Convention, *supra* note 17; Guidelines, *supra* note 11.

67 *See infra* note 141 and accompanying text.

68 Convention, *supra* note 17, art. 1.

69 The UN Guidelines adopts a broader clause. It says that "information should be able to circulate as freely as [possible]." U.N. Guidelines, *supra* note 23.

70 Guidelines, *supra* note 11.

71 *Id.*

data held by legal persons should be protected or not.[72] The Convention states that it also applies to information relating to "groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality."[73]

The OECD Guidelines aim to protect personal data.[74] However, some scholars have argued that the flexibility provided in paragraph three of the Guidelines suggests an extension to the protection of data concerning legal persons.[75] Although the protection of data concerning legal persons[76] is a very interesting issue, this Article does not address it in further detail.

c. Content of the TDF International Instruments

Among the substantive provisions contained in the COE Convention and the OECD Guidelines, there are two of great importance. One is the enumeration of a core of principles, and the other is an adoption of "special rules on TDF."

i. Principles

The core of principles on TDF establishes a minimum standard of protection of personal data that parties should adopt. It is important to mention that the broad terms used in formulating the principles provide information laws with flexibility, which has been urged[77] because of changing technology and the emergence of new problems.[78] Most of the principles are adopted in very similar terms in both instruments. However, there are some slight differences that should be noted.

The domestic acts[79] and the drafts on data protection provide a

---

[72] Some scholars argue that the Convention has adopted a compromise clause to solve this issue. *See* Garzon Clariana, *supra* note 17, at 16-17.

[73] This is how it is stated in art. 3, § 2b of the Convention. *See* Convention, *supra* note 17.

[74] *See* Guidelines, *supra* note 11.

[75] Paragraph 3 does not contain any explicit reference to legal persons. However, the Explanatory Memorandum states "protection may be afforded to data relating to groups and similar entities whereas such protection is completely nonexistent in another country." *See* Bing, *The Council of Europe Convention and the OECD Guidelines on Data Protection*, 5 MICH. Y.B. INT'L LEGAL STUD. 271 (1984).

[76] For a study in the domestic field of the constitutional protection granted to corporations, see Damrosch, *Foreign States and the Constitution*, 73 VA. L. REV. 483 (1987).

[77] *See* Kirby, *The Ten Information Commandments*, TDR, June 1986, at 19, 20.

[78] Due to the rapid advancement in the field and because of the Convention's binding nature, the Convention could become obsolete quickly. *See* Comment, *Transborder Data Flow: Problems with the Council of Europe Convention, or Protecting States from Protectionism*, 4 NW. J. INT'L L.& BUS. 601, at 625 (1982). However, it is important to highlight that the most recent laws enacted have adopted most of the general principles formulated in the COE Convention and OECD Guidelines.

[79] Besides the acts mentioned in *supra* note 56, there are other data protection acts such as: Australia: Privacy Act no. 119 (1988); Canada: Privacy Act (1987); Finland: Data

fair idea of how well the principles enumerated in the COE Convention and in the OECD Guidelines have been adopted by a variety of civilized nations.[80] Thus, the fact that those principles have become part of some domestic practice[81] demonstrates how important they have become within the international community.

There are ten basic principles specifically listed in the COE Convention and OECD Guidelines.

Collection limitation principle. The collection of personal data should be restricted to the minimum amount necessary. "[S]uch data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject" or with the authority of law (i.e. data commissioner).[82] It is important to note that only the Convention mentions a special category of data[83] that may not be processed automatically unless domestic laws pro-

---

Protection Act (1987); Guernsey: Data Protection Act (1986); Iceland: Systematic Recording of Personal Data Act (1981); Ireland: Data Protection Act no. 25 (1988); Israel: Protection of Privacy Act (1981); Jersey: Data Protection Act (1987); The Netherlands: Data Protection Act (1988); United Kingdom: Data Protection Act (1984). In the United States, a House bill calls for the establishment of a U.S. Data Protection Board. *United States: Congress Considers Data Protection Board*, TDR, June/July 1990, at 27. Its functions would be:

> (1) to develop model guidelines and regulations for use by federal agencies to implement the Privacy Act of 1974; (2) to develop guidelines for use by federal, state and local agencies; (3) to make recommendations on amending the Privacy Act of 1974; (4) to invest compliance with the Privacy Act and (5) to conduct research and investigations into matters relating to data protection.

Id.

[80] For a thorough comparative study on the principles adopted by domestic laws on data protection, see Kirby, *TDF and the Basic Rules of Data*, 16 STAN.J. INT'L L. 28 (1980).

Prof. De Miguel Castaño argues that as a result of the adoption in domestic law of the principles enumerated in the COE Convention and the OECD Guidelines it is possible to formulate general principles regarding privacy protection: "of all the legal dispositions, norms, etc., if some common *principles* can be extracted, . . . it is the protection of the intimacy in relation with the facts stored in files." De Miguel Castaño, *Derecho a la Intimidad Frente al Derecho a la Información: El Ordenador y las Leyes de Protección de Datos*, 86 REVISTA DE LEGISLACION Y JURISPRUENCIA 353, 355 (1983) (emphasis in the original).

[81] The adoption of these principles by the domestic acts is relevant to the activities carried out by the Data Protection Commissioner created by the domestic acts. Many times national commissioners have received complaints of alleged breaches of information privacy principles. *See* PRIVACY COMMISSIONER, FIRST ANNUAL REPORT ON THE OPERATION OF THE PRIVACY ACT 37 (1989) (Austl.) [hereinafter the Australian Report]; PRIVACY COMMISSIONER, ANNUAL REPORT 1989-90 29 (1990) (Can.) [hereinafter the Canadian Report]; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, 9TH RAPPORT AU PRÉSIDENT DE LA RÉPUBLIQUE ET AU PARLEMENT 1988 15 (1989) (Fr.) [hereinafter the French Report]; DATA PROTECTION COMMISSIONER, FIRST ANNUAL REPORT 17 (1989) (Ir.) [hereinafter the Irish Report]; DATA PROTECTION REGISTER, FIFTH REPORT 11 (1989) (Eng.) [hereinafter the British Report].

[82] Guidelines, *supra* note 11, § 7, at 10. The Convention states: "Personal data undergoing automatic processing shall be obtained and processed fairly and lawfully." Convention, *supra* note 17, art. 5(a).

[83] The special categories of data include: "data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life . . . and data relating to criminal convictions." Convention, *supra* note 17, art. 6.

viding appropriate safeguards are followed.[84] The OECD Expert Group explained that this special category of data was not included because it would be impossible to agree on what data was "specially sensitive".[85] However, the OECD Guidelines provide for the possibility of limiting the collection of personal data[86] without further specification.

The UN Guidelines state the same principle, adding that the information about persons should not be used for ends contrary to the purposes and principles of the Charter of the United Nations.[87]

Information quality principle. In accordance with the purposes for which it is used, personal data should be accurate, complete, and current.[88]

Purpose specification principle. The purpose for which personal data are collected should be specified, and the data should not be used in a manner incompatible with those purposes.[89] The COE Convention requires that the storage must be done for "legitimate purposes,"[90] while the OECD Guidelines do not mention legitimate purposes. Instead, the OECD Guidelines require that the purpose of the collection "be specified not later than the time of data collection,"[91] and that the subsequent use cannot be for purposes other than those specified.

The UN Guidelines include under the heading "principle of purpose-specification" the following principles: time limitation, use and disclosure, openness, and social justification.[92]

Use or disclosure limitation principle. Personal data should not be disclosed or made available except with the consent of the data subject or the authority of law, or pursuant to a publicly known usage of common and routine practice. This is the formulation as provided in the OECD Guidelines.[93] Although this principle also appears in the

---

[84] The special categories of data include those referring to racial origin, political opinions, religious or other beliefs, and data concerning health or sexual life. *Id.*

[85] Guidelines, *supra* note 11.

[86] "There should be limits to the collection of personal data." Guidelines, *supra* note 11, § 7, at 10. Section 17 of the Guidelines mentions that "[a] Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection." *Id.* at § 17, at 11-12.

[87] *See* U.N. Guidelines, *supra* note 23.

[88] "Personal data undergoing automatic processing shall be adequate, relevant and not excessive in relation to the purposes for which they are stored." Convention, *supra* note 17, art. 5 (c). "Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for the purposes, should be accurate, complete and kept up-to-date." Guidelines, *supra* note 11, § 8, at 10.

[89] Convention, *supra* note 17, art. 5(b). Guidelines, *supra* note 11, § 9, at 10.

[90] Convention, *supra* note 17, art. 5(b).

[91] Guidelines, *supra* note 11, § 9.

[92] *See* U.N. Guidelines, *supra* note 23.

[93] "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the con-

COE Convention, it is hardly substantive; the COE Convention only requires that automatically processed personal data be stored for specified and legitimate purposes and not used in a way *incompatible with those purposes*.[94]

Security safeguards principle. Personal data should be protected by security safeguards to prevent loss, destruction, alteration, dissemination, or unauthorized access.[95] The OECD Guidelines require a test of *reasonableness* on the security measures, which is not required by the Convention.[96]

The UN Guidelines suggest that it is necessary to take measures to protect files against both natural dangers and unauthorized access or fraudulent use of data.

Openness principle. There should be a general policy of openness about developments, practices, and policies with respect to personal data. In particular, means should be available to establish the existence, purposes, policies, and practices associated with personal data, as well as the identity and residence of the data controller. This principle is asserted in the OECD Guidelines.[97] The Convention, however, refers to this principle as the right of any person to establish the existence of and main purposes of an automated personal data file, as well as the identity of and habitual residence of the controller of the file.[98]

Accountability principle. With respect to any personal data record, there should be an identifiable data controller who is accountable in law for giving effect to these principles. The Convention states such principle in the course of defining the controller of the file.[99] It should be a "natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them."[100] The OECD Guidelines simply adopt the accountability of the data controller.[101]

Individual participation principle. This has been described as the "golden rule" of data protection. It establishes that an individual

---

sent of the data subject; or b) by the authority of law." Guidelines, *supra* note 11, § 9, at 10.

94 Convention, *supra* note 17, art. 5(b).

95 Guidelines, *supra* note 11, § 11, at 10. Convention, *supra* note 17, art. 7.

96 The Guidelines state that "[p]ersonal data should be protected by reasonable security safeguards." Guidelines, *supra* note 11, § 11. The Convention simply states, "[a]ppropriate security measures shall be taken." Convention, *supra* note 17, art. 7.

97 Guidelines, *supra* note 11, § 12, at 11.

98 Convention, *supra* note 17, art. 8(a).

99 *Id.*, art. 2(d).

100 *Id.*, art. 8(a).

101 Guidelines, *supra* note 11, § 14, at 11. "A data controller should be accountable for complying with measures which give effect to the principle stated above." *Id.*

should have a right: a) to obtain from the data controller confirmation of whether he has data relating to the individual; b) to learn what data relates to him within a reasonable time, in a reasonable manner, and in a form that is intelligible to him; c) to challenge data relating to him, and if the challenge is successful, to have the data corrected, completed, amended, annotated, or, if appropriate, erased; and d) to be notified of the reasons for the denial of a request made under paragraphs a) and b) and to challenge such denial. The difference of this principle as adopted by the COE Convention[102] and in the OECD Guidelines rests in the degree of emphasis each places on specific points.[103]

The UN Guidelines adopt this principle using almost the same terms as those of the OECD Guidelines and the COE Convention.[104]

Social justification principle. The collection of personal data should be for general purposes and specific uses that are socially acceptable.[105] The OECD Guidelines do not state this principle. It has been argued that the COE Convention acknowledges this principle as part of the requirement of storing data for legitimate purposes.[106]

Time limitation principle. Personal data must be "preserved in a form that permits identification of the data subject for no longer than the amount of time necessary for the purpose for which those data

---

[102] Any person shall be enabled: a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention; d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Convention, *supra* note 17, art. 8.

[103] Section 13 of the Guidelines states:

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

i) within a reasonable time;

ii) at a charge, if any, that is not excessive;

iii) in a reasonable manner; and

iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs a) and b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Guidelines, *supra* note 11, § 13, at 11.

[104] Compare U.N. Guidelines, *supra* note 23; Convention, *supra* note 17; and Guidelines, *supra* note 11.

[105] Convention, *supra* note 17, art. 5(b).

[106] "[P]ersonal data undergoing automatic processing shall be stored for . . . legitimate purposes." *Id.*

are stored."[107] This principle does not appear in the OECD Guidelines.

Alternative principles outside of the OECD Guidelines and COE Convention. The UN Guidelines also include a principle of non-discrimination. This means that any exceptions (allowed by this instrument) made to the above-referenced principles cannot give rise to arbitrary discrimination.[108]

Both the COE Convention and the OECD Guidelines foresee the possibility that these basic principles are sometimes restricted. Such derogations are sometimes allowed as necessary measures in a democratic society to protect national security, public safety, monetary interests of the state, or the suppression of criminal offenses.[109] The OECD Guidelines refer to these exceptions— national sovereignty, national security and public policy—as "public order" exceptions.[110] However, the Guidelines add that there should be as few exceptions as possible and that exceptions should be made known to the public.[111]

The UN Guidelines also state some exceptions to these principles. Among those are: the protection of national security, public order, public health and morality, the rights and freedoms of others, and the promotion of humanitarian assistance.[112] However, these exceptions are limited by the provisions prescribed by the Universal Declaration of Human Rights and the other relevant instruments in the field of the protection of human rights and the prevention of discrimination.[113]

The Convention and the Guidelines are the first international instruments[114] to state some general principles that should apply to the transmission of personal data. Furthermore, the adoption of most principles, as well as the objectives pursued by the COE Convention and the OECD Guidelines, by the existing national data protection acts[115] is an important step to consider. Even though all domestic data protection laws do not have the same scope, they have adopted the principles in a manner appropriate for their purpose. For instance, some of the national acts, such as the Canadian Privacy

---

107 *Id.* art. 5(e).

108 The arbitrary discrimination, according to the U.N. Guidelines, includes: "information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union." U.N. Guidelines, *supra* note 23.

109 Convention, *supra* note 17, art. 9, § 2.

110 Guidelines, *supra* note 11, § 4.

111 *Id.*

112 U.N. Guidelines, *supra* note 23.

113 *Id.*

114 *See supra* notes 57-62 and accompanying text for the different legal nature of these instruments.

115 *See supra* notes 56, 79.

Act,[116] are enacted to provide access to information under the control of public authorities. Others, such as the Danish Act,[117] include not only natural persons but also legal persons.

The UN Guidelines have added some relevant provisions on the formulation of the principles to those of the OECD and COE. Among them are non-discrimination as a separate principle in the transmission of information and a reference to the UDHR and other human rights international instruments as limits on the power to make exceptions to the principles. Finally, the UN Guidelines give special attention to the collection and processing of data according to the purposes and principles of the Charter.[118]

It is possible that if the above principles were formulated in a more flexible way, they could be extended to regulate transborder flow of non-personal data as well. In that event, it may be necessary to add additional standards in order to allow the extension of TDF's principles to other areas of data protection. For example, it seems convenient that the scope of the security safeguards principle would cover not only personal data, but also economic data. A reasonableness criteria could determine to what extent the above-mentioned principles could be formulated in more general terms.

ii. Special Rules on TDF

The protection of personal data and personal privacy in the COE Convention and the OECD Guidelines is accomplished not only by listing the mentioned principles, but also by regulating the transfer of personal data across national borders.[119]

The fear that the COE Convention would be used by some countries as an instrument to interfere with the free flow of information caused the drafters to include the following prohibition:

> a Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party.[120]

---

[116] *Supra* note 79; the United States Privacy Act covers data collected and processed by the Federal government only. 5 U.S.C. § 522(a) (1976). Individuals are given a right of access to this data. *Id.* Some states, such as New York, have enacted similar laws covering records held by state agencies. *See* R. SMITH, COMPILATION OF STATES AND FEDERAL PRIVACY LAWS (1985). All European data protection laws cover the public and private sectors, and give data subjects a right of access to records concerning themselves, together with a right of correction, or a right to file a note of disagreement. *See supra* note 56. On access to data, see Burkert, *Data Protection and Access To Data*, in FROM DATA PROTECTION TO KNOWLEDGE MACHINES 49 (Seipel ed. 1990).

[117] *See supra* note 56 and accompanying text for other examples.

[118] U.N. Guidelines, *supra* note 23.

[119] Convention, *supra* note 17, art. 12. Guidelines, *supra* note 11, §§ 15-18, at 11-12.

[120] Convention, *supra* note 17, art. 12, § 2. Similar terms are used in the Guidelines: "Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection." Guidelines, *supra* note 11, § 18, at 12.

However, some provisions contain the following exceptions to this clause: (i) subject related exceptions, or the "special categories of data"; (ii) the most important exception—when the other party provides *equivalent data protection*; and (iii) transfers made through another country not party to the Convention with the purpose of evading the regulations of the Convention.[121] Despite these exceptions, this clause is important because it asserts the notion of a free flow of information, at least among countries with data protection laws.

The equivalent or reciprocity clause[122] has been a source of controversy among scholars.[123] Some express a fear that the equivalent clause would increase restrictions on data flows,[124] since a country with strict standards could refuse to transfer data to any country with less protective standards. Since the Convention entered into force in 1985, refusals to transfer data to other countries were based on the lack of legislation on data protection in the transferee country, and not on the inferiority of the standards provided by their data protection legislation.[125]

The equivalent clause has induced some action by the Consultative Committee, which was set up after the Convention entered into force. The problem raised by the equivalent clause is not related to its general acceptance, but to the interpretations given its content. Thus, the Consultative Committee has requested that member states report on their interpretations of the equivalent clause.[126] Some scholars have tried to overcome the difficulties and worries raised by the equivalent clause with contractual solutions.[127] However, such solutions may be adequate in certain cases, but they do not provide a general solution.[128]

In addition, the UN Guidelines have tried to clarify, although

---

[121] Convention, *supra* note 17, art. 12.

[122] Convention, *supra* note 17, art. 12, § 3.

[123] *See* Comment, *supra* note 78, at 622. *See also* Nutger, TRANSBORDER FLOW OF PERSONAL DATA WITHIN THE EEC (1990).

[124] *Id.*

[125] For example, France denied approval of the transfer of personal data to the headquarters of Fiat in Turin (Italy). *No Fiat for Fiat*, TDR, Nov. 1989, at 10. The argument was based on the ground that Italy had not ratified the Convention. *Id.* However, the French institution on data protection accepted the commitment of the Italian headquarters to apply the full protection of human rights and fundamental liberties awarded by the Convention and the French Act [hereinafter cited as the Fiat case]. *Id.* Italy has still not ratified the COE Convention.

Another example would be France's refusal to approve the transfer of data on Spanish civil war prisoners to Spain. *Commissioners Stress TDF Risks*, *supra* note 31. Although both countries had ratified the Convention, the French authorities argued that Spain had not implemented the Convention into its domestic laws and therefore that Spain lacked the protection required for such data. *Id.*

[126] French Annual Report, *supra* note 81, at 46.

[127] Napier, *supra* note 3, at 17.

[128] *See* J. Bing, Reflections on a Data Protection Policy for 1992 14 (1990) (Paper presented at a conference on "Access to Public Sector Information, Data Protection and Computer Crime" held in Luxembourg, March 27-28, 1990). .

unsuccessfully, the meaning of the equivalent clause. The reference to the ". . . more or less equivalent safeguards . . ." does not provide a satisfactory solution to how the equivalent standards should be defined.[129]

It is obvious that, as in any treaty or convention, the only way to avoid ambiguities is by adopting very specific provisions. However, the novelty of TDF required, at that time, a flexible framework with broad principles and provisions.

iii. Other provisions

Since the Convention is non self-executing,[130] it requires that its principles be adopted and complemented by domestic binding norms. The Convention expressly states that it is possible for a party to grant data subjects a "wider measure of protectionism than that stipulated" in the Convention.[131] Both the COE Convention and the OECD Guidelines impose a duty on the parties to implement domestically the principles stated in both instruments and to establish legal, administrative, and other procedures or institutions to protect both privacy and other individual liberties with respect to personal data.[132]

In addition to the provisions in the COE Convention for cooperation between parties and mutual assistance on its implementation, the Convention also creates a Consultative Committee.[133] This Committee functions to facilitate the application of the Convention, to express an opinion at the request of the parties on any question concerning the application of the Convention, and to propose amendments to the Convention as established in its articles.[134]

The OECD Guidelines provide for both international cooperation between member states to facilitate information exchange related to the Guidelines and for mutual assistance in the procedural matters involved.[135] In addition, the Guidelines recommend the es-

---

129 U.N. Guidelines, *supra* note 23, § 11.

130 *See* Garzon Clariana, *supra* note 17, at 18; Rigaux, *La Loi Applicable à la Protection des Individus à l'égard du Traitement Automatisé des Donnés à Caractére Personnel*, 69 REVUE CRITIQUE DE DROIT INTERNATIONAL PRIVÉ 443 (1980).

131 Convention, *supra* note 17, art. 1.

132 The Convention states that "[e]ach Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party." Convention, *supra* note 17, art. 4. The Guidelines state, "In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data." Guidelines, *supra* note 11, § 19, at 12.

133 Convention, *supra* note 17, art. 19.

134 *Id.* The norms on the Procedure for the election and constitution of the Committee are established in article 20. *See id.*, art. 20.

135 Guidelines, *supra* note 11, §§ 20-22, at 12.

tablishment of institutions for the protection of privacy and other individual liberties with respect to personal data.[136]

The UN Guidelines also recommend that states designate an authority competent to supervise the observance of these guidelines. In this author's opinion, the UN is the appropriate international organization for setting up a Consultative Committee to assist the states with the implementation of their data protection acts, to gather all the new and updated national acts and annual reports on data protection, and more importantly, to work together with the national data commissioners toward a binding international instrument on TDF concerning personal data.

Finally, the COE has been criticized for its regional character. However, its inclusion of a final clause inviting non-member states to accede to the Convention[137] provides an international dimension. Even though the Convention was a product of the European experience with TDF,[138] it is difficult to deny that its influence reaches beyond the European context.[139]

2. *OECD Declaration on TDF*

a. *Negotiation and Content*

Negotiation. After the Guidelines recognized that the protection of privacy could be a justifiable reason to limit TDF, the business community urged the OECD member states to allow the free flow and access of information across borders.[140] The private sector made it clear how important TDF of personal and non-personal data was for their world-wide operations.[141]

---

[136] *Id.*, § 19, at 12.

[137] This invitation is subject to some requirements such as the entry into force of the Convention and that the invitation has to be formally made by a decision of the Council of Europe. Convention, *supra* note 17. Article 23 of the Convention reads: "After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee." *Id.* It is expected that some of the Eastern European countries will accede to the Convention. *See infra* note 268 and accompanying text.

[138] Jacqué, *La Convention pour la Protection des Personnes a l'Egard du Traitement Informatisé des Données a Caractère Personnel*, 26 ANNUAIRE FRANÇAIS DE DROIT INTERNATIONAL 773, 785 (1980).

[139] *See infra* notes 261, 268 and accompaying text.

[140] *See Governments and Companies Seek TDF Cooperation*, 7 TDR 26 (1984).

[141] The Vice-President of the American Express Company has referred to the importance of TDF to his organization:

> American Express, like other multinational corporations and especially service sector corporations relies on automated, reliable and cost-effective global communication networks for the majority of its international operations. . . . Communications are also essential for other internal operations: personnel records, in-house communications lines, internal budgetary-procedures, . . . all depend on our ability to transmit and store information within and across international boundaries. Finally, but very significantly as a

The formulation of the Declaration was mitigated by terms much more moderate than those proposed by some countries. For instance, the French approach was to adopt a broad document that would deal with the different types of information flows. Other parties, such as the United States, were eager to reach a multilateral commitment that would include a formulation on access to data resources.[142] The rest of the member states felt the need to adopt some rules on TDF but failed to express a strong position.

Throughout the negotiation process, the commitments contained in the Declaration were weakened. The initial draft recognized the unrestricted flow of data as an absolute value. In contrast, the final text of the Declaration states that there are other competing values which do not necessarily need to be of fundamental nature, but which can compete with national law and politics.[143] The final text of the Declaration does however, successfully advance the free flow of information.[144]

Content. The OECD Declaration on TDF—the first multilateral instrument dealing with TDF of non-personal data—reflected the interest of the member states in recognizing the economic importance of TDF.[145] In general, a declaration constitutes a "solemn form of understanding on principles, without stipulating strict commitment on behalf of the participating parties."[146] The OECD Declaration on TDF can be characterized as establishing a minimum platform for developed countries on the negotiations of services.[147] No strict commitments were made.

The Declaration contains three sections. The first section states a series of general facts related to computerized data and international information flow.[148] Thus, it recognizes that in spite of the different benefits member states receive from TDF, it is important to develop common approaches and to harmonize solutions addressing all issues of TDF.

The second section states the intentions, classified in four differ-

---

result of these operations, American Express hold [sic] a vast amount of confidential information on our customers.

Transborder Data Flows: The European Convention and United Kingdom Legislation, 35 INT'L & COMP. L.Q. 710, 713 (1986) (quoting U.S. NATIONAL COMMITTEE OF THE INTERNATIONAL INSTITUTE OF COMMUNICATIONS, COMMUNICATIONS AND INTERNATIONAL TRADE: A SYMPOSIUM 4 (1982)).

142 *See generally* K. SAUVANT, *supra* note 48, at 243.

143 "Recognizing that national policies which affect transborder data flows reflect a range of social and economic goals, and that governments may adopt different means to achieve their policy goals . . . ." Declaration, *supra* note 12, at 88.

144 *Id.*

145 *Id.*

146 Vogelaar, *supra* note 59, at 136.

147 Declaration, *supra* note 12.

148 *Id.* § a.

ent categories, that are to be carried out by the signatory parties.[149] The first of these categories—and most important— seeks to balance the access to data with the creation of unjustified barriers to the international exchange of data. Indeed, the inclusion of the accessibility to data is very important because it provides an extra ground for a request filed by a country seeking access to important information stored in the data bases of another country.[150] The second category states the intention to seek transparency in regulations and policies relating to information.[151] The third category sets forth the intention not only to develop common approaches on issues related to TDF, but also to reach harmonized solutions.[152] The fourth category expresses the need to be considered with other countries' implications on TDF.[153]

The final section of the Declaration deals with the work that will be undertaken by the signatory parties on TDF.[154] Privacy aspects are left aside, while the commercial and economic concerns of TDF are stressed. As the French proposal suggested at the beginning of the negotiation process, other types of data flow with economic implications should be studied in depth. Thus, the agenda for the OECD member countries listed the following issues: a) flows of data accompanying international trade; b) marketed computer services and computerized information services; and c) intra-corporate data flows.

Obviously those are not simple issues of discussion, because many interests are involved. However, the completion of such an enterprise would be very important to the achievement of a uniform international practice on TDF of non-personal data.[155]

b. Legal Nature

The legal nature and the effects of the OECD Declaration are among the most interesting problems for discussion. Before doing

---

149 *Id.* § b.

150 Canada specifically requested the clause's inclusion, a fact which reflects Canada's particular concern for its increasing dependency on data located elsewhere and its resulting vulnerability. *See* K. SAUVANT, *supra* note 48.

151 Declaration, *supra* note 12, § b.

152 *Id.*

153 *Id.*

154 *Id.* § c.

155 It is necessary for the international community that cases such as *Dresser* do not reappear. Dresser, a major U.S. supplier of oil field, pipeline equipment and related technology, was required to comply with orders of the U.S. export-control authorities in regard to the export of goods produced by its subsidiary in France with U.S. technology. Kincannon, *The Dresser Case: One Step Too Far*, 5 N.Y.L. SCH. J. INT'L & COMP. L. 191, 202-04 (1984). Dresser had to comply with the government's embargo of technology exports to the Soviet Union and had to change the entry key to a computer in Pittsburgh. *Id.* at 204. That barred Dresser's French subsidiary from access to the technology it needed, and without such access to Dresser's computerized data bank, Dresser-France's engineers lacked vital information to run the company's business. *Id.*

so, it should be noted that the Convention by which the OECD was created does not mention the "declaration" as a form within the decisional process of the organization. Furthermore, the "declaration" form has been developed by the organization in response to the need for a more flexible means for majority actions.[156] However, its effect is the same as that of the Council decisions, because once a declaration is adopted by the Group of Experts, it is submitted to the Council for its adoption and only then becomes integrated in the structure of the organization. Thus, it could be argued that the "declaration constitutes an international agreement" establishing specific and basic principles.[157]

As the analysis of the TDF Declaration has shown, there is no enforceable mechanism in the prescribed rules. However, the Declaration constitutes a source of law and its legal effects are significant. It is obvious that, if the Declaration constituted a declaration of rules of customary international law, then its binding force would not be questioned. Even though this point is discussed in further detail in the next section, it is important to note that the doctrine has accepted a "status nascendi" on a TDF custom.[158]

The fact that the Declaration is not a declaratory document on existing customary law does not necessarily mean that its legal effects are nil. Some scholars have characterized this kind of non-binding rule contained in guidelines or declarations as "soft-law." In areas such as international economic relations[159] or environmental law,[160] some rules are still controversial. Nevertheless, international instruments have been enacted containing rules that compensate for inequalities between countries. Although these rules have been considered law "without legal obligations"[161] because they lack enforceable rules, they have some effects that cannot be ignored. Thus, the acceptance of "soft-law" would justify somehow the steps

---

156 In reality, declarations are acts of governments in the OECD framework, but not an act of the organization. The Ministers who issue the declaration do not act as members of the Council.

157 Vogelaar, when talking about the Guidelines on MNC which took the form of a declaration, said: "Declaration[s] [constitut]e an international agreement (source of international law) on basic principles of investment policy and on proceedings to implement these." Vogelaar, *supra* note 59, at 134.

158 Some authors have argued that the Declaration contributes to the evolution of customary international law while others argue that such events may happen eventually. *See* K. SAUVANT, *supra* note 48, at 244. Piñol Rull, *Los Flujos Internacionales de Datos: Aproximacion a su Regulatión Jurídica*, 4 UNIVERSIDAD NACIONAL DE EDUCACION A DISTSACIA 146 (1987); Grewlich, *supra* note 13, at 14.

159 Seidl-Hohenveldern, *International Economic Soft-Law*, 163 RECUEIL DES COURS 169, 194 (1979).

160 *See* Dupuy, *Cours General de Droit International Public*, 165 RECUEIL DES COURS 182 (1979).

161 *See* Roessler, *Law, de Facto Agreements and Declarations of Principle in International Economic Relations*, 21 GERMAN Y.B. INT'L L. 39, 41 (1978).

taken in accordance with the principles accepted therein.[162] Furthermore, the principles embodied in the declarations have acquired a "standstill effect;"[163] the states that have accepted them cannot act in a way contrary to those principles unless it is justified by a fundamental change of circumstances.[164]

B. International Custom Applicable to TDF

The question of whether an international custom on TDF of non-personal data exists has been answered by legal doctrine.[165] Although this point is addressed briefly, this Article's analysis of international custom is focused on TDF containing personal data.

To approach this issue properly, it is necessary to analyze the relevance of the multilateral instruments on TDF to the formation of custom. It is important to note that international instruments dealing with TDF have a dual approach: one with respect to TDF of personal data (this is the case of the Convention and the OECD Guidelines), and another regarding TDF of non-personal data (this is the case of the Declaration). Another issue analyzed in this section is the possibility that, because of the different geographical dimensions of those instruments, the custom on TDF is consolidated more regionally than internationally.

Article 38 (1) (b) of the Statute of the International Court of Justice (ICJ) refers to international custom as "evidence of a general practice accepted as law."[166] From that statement it is clear that the definition of custom comprises two elements: (i) general practice by the states and (ii) acceptance of this practice by states as law. Since the *Lotus* case,[167] the ICJ has adopted the position that an international custom needs to fulfill an objective requirement formed by the state practice, and a subjective requirement related to the opinio

---

162 Dupuy, *Droit declaratoire et droit programmatoire: de la coutume sauvage à la 'soft-law'* in L'ELABORATION DU DROIT INTERNATIONAL PUBLIC 133 (1975).

163 *See* Seidl-Hohenveldern, *supra* note 159.

164 *See* article 62 of the Vienna Convention on the Law of Treaties, UN. Doc. A/CONF.39/27 (1969).

165 This custom is phrased in the following terms: "it reflects a careful balance between access to data and information and the removal of unjustified barriers to the international exchange of data and information." Grewlich, *supra* note 13. It has been said that such a custom has exclusively a "status nascendi." *See* Rull, *supra* note 158, at 146; K. SAUVANT, *supra* note 48, at 246.

166 Statute of the International Court of Justice, 59 Stat. 1055, T.S. 993 (1945).

167 The Case of the S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No.10 at 28 (Sept. 7); North Sea Continental Shelf Cases (Den. v. W. Ger.), 1969 I.C.J. 4. The Asylum case stresses the need of opinio juris for the existence of an international custom. Asylum Case (Colum. v. Peru), 1950 I.C.J. 266 (Judgement of Apr. 12). In the Nicaragua case, the Court has reiterated the requirement of the existence of state practice and opinio juris. Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), 1986 I.C.J. 14. *See* Marek, *Le Probleme des Sources du Droit International dans l'Arret sur le Plateau Continental de la Mer du Nord*, 8 REVUE BELGE DE DROIT INTERNATIONAL 55 (1970-71).

juris or consent of the states. Thus, it is necessary to determine whether TDF fulfills these requirements.

Prior to addressing these questions, the content of this purported international custom that involves TDF concerning personal data must be considered. Content refers to the existence of a restriction on TDF concerning personal data unless protections similar or equivalent to those of the transferor country exist in the recipient country. To define content in positive terms, one could say that there is a free flow of personal data between those countries with reciprocal safeguards and limitations.

This custom is in accordance with the purpose of the COE Convention and the OECD Guidelines to achieve a free flow of information between people by removing unjustified barriers. The UN Guidelines also express this notion in similar terms.

1. Objective Element: Practice

According to the ICJ, a constant and uniform state practice is necessary to give rise to a rule of customary law.[168] When discussing the objective requisite on TDF issues, questions arise as to what kind of practice is necessary to fulfill the requirements of constancy and uniformity; whether state practice includes enactment of national legislation as well as the duties of the national Data Commissioner; how constant must constant practice be; and whether a "short period" of practice is sufficient if the practice involves rapidly developing technology, such as TDF.[169]

a. Manifestation of the Practice

Although only states are considered subjects of international law and therefore are able to create customary law, international organizations may participate in the creation of such customs.[170] Both the COE and the OECD have made important contributions to the regulation of TDF. Because they are composed of representatives of states, for purposes of this Article their practices shall be included in state practice.[171]

---

[168] Right of Passage over Indian Territory (Port. v. India), 1960 I.C.J. 6 (Judgement of Apr. 12) (case concerning right of passage over Indian territory). In the Asylum Case, the ICJ said that there was no customary rule because the practice was neither constant nor uniform. *Supra* note 167.

[169] The requirement of constant practice is linked to a time element. If practice requires a certain repetition of acts, then time is needed. *See* Akehurst, *Custom as a Source of International Law*, 37 BRIT. Y.B. 11, 15 (1974-75).

[170] *See* Guidelines, *supra* note 11j Convention, *supra* note 17.

[171] *See generally* Wolfke, *Practice of International Organizations and Customary Law*, 1 POLISH Y.B. INT'L L. 183 (1966-67). Akehurst states, "it is true that most organs of most international organizations are composed of representatives of states, and that their practice is best regarded as the practice of states." Akehurst, *supra* note 169, at 11. Professor Garzon Clariana says that the state has maintained an important role within the decision making

The practice on data protection which, until now, had been conducted by sovereign states, entailed a variety of forms[172] and different levels of repetitions.[173] Before the multilateral instruments on data protection had been adopted, some countries had already enacted domestic laws[174] or were preparing drafts of such laws.[175] Since the COE and OECD multilateral instruments have been adopted, many countries have enacted or have modified their domestic laws on data protection[176] in order to be in accordance with the provisions and principles set forth in these instruments.

Most of the rules on TDF adopted in the data protection acts differ in their content according to the data protection system of each country. For example, in some cases, TDF has to be approved, licensed, or registered, or some material regulations must be observed.[177] However, the general notion that prevails is the same: the assurance that, once personal data is sent abroad, it receives protec-

---

process of most international organizations through their vote. Garzon Clariana, *El Valor Jurídico de las Declaraciones de la Asamblea General de las Naciones Unidas: Valor como Recomendaciones—declaraciones y Actos Estatales*, 11 REVISTA JURÍDICA DE CATALUÑA 901, 903 (1973). Professor Diez de Velasco Vallejo states that it is sometimes hard to know whether international organizations are fulfilling the provisions of their constitutive treaty or whether they are creating an international custom. Diez de Velasco Vallejo, 1 INSTITUCIONES DE DERECHO INTERNACIONAL PUBLICO 85 (1986).

172 "State practice means any act or statement by a State from which views about customary law can be inferred; it includes physical acts, claims, declarations *in abstract* (such as General Assembly resolutions), national laws, national judgments and omissions." Akehurst, *supra* note 169, at 53 (emphasis in the original). Several articles have extensively discussed whether ratification and accession to treaties constitute state practice. Schachter, *Entangled Treaty and Custom* in INTERNATIONAL LAW AT A TIME OF PERPLEXITY 717 (1989). *See* H.W.A. THIRLWAY, INTERNATIONAL CUSTOMARY LAW AND CODIFICATION (1972).

173 "As regards the quantity of practice needed to create a customary rule, the number of States participating is more important than the frequency or duration of the practice. Even a practice followed by a few States, on a few occasions and for a short period of time, can create a customary rule." Akehurst, *supra* note 169, at 53.

174 *See supra* notes 56 and 79.

175 An example is the proposed Spanish data protection act which has been a subject of discussion since 1979.

176 For example, Finland passed a Personal Data Files Act in April of 1987. *Finland*, TDR, Nov. 1989, at 9. Hungary adopted its Data Protection Bill in 1989. *See Hungary to Enact Data Protection Law*, TDR, Nov. 1989, at 6 and Sólyom, *Hungary: New Data Protection Rights*, TDR, Nov. 1989, at 29.

Other countries, such as Sweden and Portugal, have added new provisions to their constitutions safeguarding the privacy of the individual when automatic data processing is used. *See Sweden*, TDR, Nov. 1989, at 16; *Portugal: New Constitution Protects Personal Data*, TDR, June/July 1989, at 28. In the Spanish Constitution of 1978, article 18, section 4 provides for the protection of the individual privacy by establishing some requirements to the computerized sending of data. For a thorough study on this subject, see Garzon Clariana, *La Protectión Jurídica de Datos de Character Personal*, in LAS IMPLICATIONES SOCIALES DE LA INFORMATIÓN (1980).

177 *See supra* note 156. For a comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom and the Netherlands and their impact on the private sector, see Nutger, *supra* note 123. For a study on the application of data protection laws in the field of TDF, see ELGER, *European Data-Protection Laws as Non-Tariff Barriers to the Transborder Flow of Information*, in THE LAW AND ECONOMICS OF TRANSBORDER TELECOMMUNICATIONS (1987).

tion under standards similar to those guaranteed in the transferor country.[178]

In addition to the provisions on TDF included in the national data protection acts, state practice includes the activities undertaken by the national data protection authority—the data commissioner. The commissioner's role is very important because of the wide variety of functions he has.[179] Data commissioners have experienced significant increases in complaints alleging breaches of the domestic data protection acts and in applications requesting access to information concerning the requesting party.[180] Regarding commissioners' activity on TDF, there have not only been important decisions but also an increase in applications requesting permission to send information to other countries.[181] In most cases where the transfer of data was denied, the denial was based on the lack of legislation on data protection in the recipient country and on the fear that the

---

[178] The French example of the Fiat case could illustrate this point. Certain transfers of data should be subject to pre-authorization or special conditions in order to safeguard the principles of the data protection law, article 24 of the French Act on Data Processing Files and Individual Liberties 1978. *See supra* note 56; *supra* note 125. The Luxembourg Act provides that the transfer abroad of personal data is subject to the same conditions as a transfer to third parties within the country. Law of Mar. 31, 1979, art. 3(3) (Lux.). *See supra* note 56. The Irish Act provides that the transfer of personal data outside the state shall comply with the provisions of article 12 of the COE Convention. Data Protection Act, 1988, No. 25, § 11 (Ir.). *See id.* The British Act provides that the transfer of personal data abroad can be denied if the recipient state is not bound by the European Convention. Data Protection Act, 1984, § 12 (U.K.). *See supra* note 79.

[179] Their functions include initiating investigations, granting permission to access to send data across the border, hearing individual complaints and applying the fines as established in the particular act. However, every domestic act has some variation on these functions.

[180] The Danish Data Surveillance Authority's annual report of 1982 reported that the number of cases covered by the Act had increased. *See Danish Privacy Cases Increase*, TDR, Jan. 1983, at 12. It was disclosed that the authority reviewed 654 new cases. *Id.*

The Canadian Data Authority received 1,039 complaints in 1988-89 while it received 1,086 complaints in 1989-90. Canadian Annual Report 1988-89, *supra* note 81, at 29. The grounds of the complaints were: access to information; use of disclosure; correcting and updating information; time limits and collection; retention and disposal. *Id.* at 29-30.

In France, the Commission received a total of 3,673 complaints and requests on issues related to data protection in 1988. French Report, *supra* note 81. For some particular cases, see the French Report. *Id.*

According to the British Annual Report, the total number of complaints received from June 1988 to May 1989 was 1,122, and the number of complaints received in the previous twelve month period was 836. British Annual Report, *supra* note 81. Misuse of data or inaccurate data are among the common grounds for complaints. *Id.*

In Australia, since the privacy Commissioner took office in 1989, he has received 21 complaints alleging breaches of information privacy principles: collection of information, storage of information and access to it, accuracy and use of information, and limits on use and disclosure. *See* Australian Annual Report *supra* note 81, at 37.

In Finland, since the Data Protection Act entered into force in 1988, the Data Protection Board has rendered forty-nine decisions concerning exceptional permissions to collect data. *See Finland*, TDR, Nov. 1989, at 9.

[181] Between July 1988 and June 1989, the Swedish Data Inspectorate Board considered about 2,700 applications for permission to send information to other countries. *Sweden*, TDR, Nov. 1989, at 16.

transferred data would not be protected.[182]

Other activities conducted by these commissioners take place in the international context, such as the organization of annual meetings. The purpose of these meetings is to discuss and inform the rest of the commissioners about their cases and problems or tensions found in their national laws, as well as to inform them how to reach an exchange of information across boundaries while guaranteeing a high standard of protection of personal data.[183]

The national courts rarely decide cases involving issues of TDF.[184] The lack of court decisions may be explained. National data protection authorities attempt to prevent claimants under national data protection acts from seeking relief in courts by stressing that judges in general do not have enough expertise in the area to make proper determinations. Instead, national data protection authorities often seek to remedy most situations through conciliation or persuasion.[185] Most discussions on data protection in general are carried out by the data authority, and very few cases reach the high courts.[186] Although national courts hear some cases that involve TDF, most involve other areas of the data protection acts, such as the liability of the keeper[187] or general aspects on the right of privacy.[188]

---

[182] The Swedish Data Inspectorate Board has refused to grant licences for the export of data to the UK. Bing, *Transnational Data Flows and the Scandinavian Data Protection Legislation*, 24 SCANDINAVIAN STUD. IN L. 71, 73 (1980). The reason for the exportation was the existence of better facilities for data processing in the UK. *Id.* The licenses were refused where the data referred to a large section of the population, and the UK did not have any data protection legislation. *Id.*

The French Commission has also denied the export of personal data in some instances, such as the Fiat case and the case of the Spanish prisoners. *See supra* note 31, at 125.

[183] At the end of these annual meetings, a Resolution is adopted with recommendations to the international organizations who have taken action on data protection, in particular on TDF, about what should be the priorities on their agenda. *See* Resolution of the 11th Conference of Data Protection Commissioners (Berlin, Aug. 30, 1989), *reprinted in* TDR, Nov. 1989, at 33. The data protection commissioners of the EEC member states provided a statement on how the Community activities on data protection should be focused. *Id.* at 34.

[184] Burkert, *Institutions of Data Protection—An Attempt at a Functional Explanation of European National Data Protection Laws*, 3 COMPUTER/ L.J. 167, 187 (1981).

[185] France and Germany are among the countries with a greater amount of litigation involving privacy legislation. See OECD, PRESENT SITUATION AND TRENDS IN PRIVACY PROTECTION IN THE OECD AREA 8 (1989).

[186] In 1988, the Constitutional Court of Austria rejected a challenge to the TDF provisions in the Data Protection Act of 1978. *Austria: Top Court Upholds TDF Rules*, TDR, Dec. 1988, at 26. The High Court held that the Data Commissioner's requirements imposed on a Swiss branch in transmitting employees' data abroad met a legitimate purpose of public interest in protecting the right of privacy. *Id.*

[187] The French Court has rendered some decisions based on the breach of art. 44 of the French Data Protection Law. In 1988, the Supreme Court of France upheld the conviction of a data bank keeper in Nantes for: (i) not properly filing with the National Commission on Informatics and Liberties his data bank on matters of personal solvency, and (ii) obstructing an inspection. *See France: Court Blows Hot/Cold on Data Case*, TDR, Mar. 1988, at 26. The District Court said that the existence of files of this nature should not

Thus it is clear that: (i) there is a certain generality and uniformity in the national legislation provisions on TDF of personal data among developed countries[189] (particularly European countries); (ii) there is uniformity in the activities undertaken by the data commissioners; and (iii) in practice, the equivalent requirement has not been used as an additional restriction or barrier on data flow among countries.[190] Certainly there is an intention to promote the removal of unjustified barriers if the information transferred is protected in the recipient countries by similar standards as those existing in the sending countries.

Aside from this intention or willingness is a practice that seeks to undertake such aims and intentions. Thus, the custom on TDF of personal data is becoming more general and uniform. There is no doubt that this practice will increase as soon as the data commissioners designated in the latest data protection acts start supervising

---

have been kept secret for the data subjects and that the data subjects should have been able to protest their inclusion. *SKF Found Guilty*, TDR, Nov. 1987, at 24.

The Swedish District Courts have awarded damages in cases where the responsible keeper was sued by persons who had suffered harm as a result of inaccuracy in the data. *Data Quality Case Costs Swedish Municipality*, TDR, Jan-Feb. 1982, at 12.

188 The West German Federal Constitutional Court declared a statute, the "Volkszaehlungsgesetz" —the "census statute"—, unconstitutional. Dippoldsmann, *Census and Judgement of the Constitutional Court in the FRG: Some Principles and Consequences*, 7 INFORMATION AGE 203, 204 (1985). The Court was concerned that the data gathered in this census was intended to be used not only for statistical purposes, but also to update information in local registration agencies. *Id.* The Court said that the citizen had a right to determine if his personal data is disclosed and how it is used. *Id.* The Court recognized that the "right of informational self-determination" is a prerequisite for the functioning of a democratic society. *Id.* at 204-05. According to this judgement, the legislator can restrict this right if it is required for the protection of public interest. *Id.* at 204. *See* Schindel, *Germany Declares Self-determination over Personal Data*, TDR, Aug.-Sep. 1984, at 359. In 1969, the West German Federal Constitutional Court developed principles concerning human dignity as part of the right to privacy— Mikrozensus. *See* Daniel-Paczosa, *Data Protection in West Germany*, 13 ARIZ. J. INT'L & COMP. L. 163 (1987).

The United States Supreme Court heard a case in which the Drug Enforcement Agency (DEA) arrested a person whose behavior matched an agency profile for suspicious individuals. United States v. Sokolow, 490 U.S. 1 (1989). The majority of the Court held that the agents of the DEA acted absolutely lawfully. *Id.* at 11. However, the dissenting opinion of Justice Marshall, who was joined by Justice Brennan, is interesting. *Id.* They argued that a non-transparent and uncontrolled processing of personal data prompts citizens to renounce their constitutional rights and adjust to the behavior followed by processing agencies according to their policies and expectations. *Id.* at 16-17. *See Data Protection: Transcending the National Agenda*, TDR, Nov. 1989, at 23, 26.

189 Brazil would be an exception. Since 1979, it has been adopting and implementing a set of policies on TDF and on underlying fields of telecommunication, informatics and telematics. *See* TRANSBORDER DATA FLOWS AND BRAZIL at 144, U.N. Doc. ST/CTC/40 (1983) [Hereinafter Study on TDF and Brazil]. The objectives of those policies have been to promote the amount of information resources located in its territory as well as to keep control over TDF and technologies relating to Brazilian industries. *Id.*

Even though other developing countries have had some approach to the dimension of TDF through the IBI organization, most of them have not adopted any domestic acts on data protection.

190 For an example of the discussion of the COE Convention's equivalent clause, see *supra* note 125.

compliance with their acts. However, the question arises whether this practice is spread throughout the international community or is located in a region or area.

As examples have shown, this practice is mainly focused within the European framework, including the EEC countries as well as other European countries. It is this author's position that the consolidation of custom has only occurred in the European context. This is probably due to the early European tradition of requesting minimum standards on personal data that had to be sent abroad. This tradition, which dates from the early 1970's, has been spread throughout Western Europe, and today is spreading to Eastern Europe.[191]

With respect to the TDF of non-personal data, the OECD Declaration reaches a balance between the free flow of information and the creation of unjustified barriers to the access of data.[192] This is an important step toward a consensus on the TDF of non-personal data.

Those cases involving transmission of non-personal data are treated very differently domestically than the TDF of personal data. In the United States, for example, the transmission or exportation of technical data would be regulated or controlled through the Export Administration Act.[193] However, in situations where enterprises are subject to discriminatory practice affecting TDF, they may be protected under the legal regime established in bilateral treaties of Friendship, Commerce and Navigation (FCN).[194] Although many bilateral treaties of FCN have been adopted, they cannot be considered as the solution to the lack of legal regulation on TDF of non-personal data. First of all, TDF is an issue that concerns the whole international community, whereas those treaties of FCN are exclusively bilateral. Secondly, some important aspects of TDF are not resolved in those treaties, such as how to determine the worth of data.

The state's willingness (as shown by the OECD Declaration) to have a uniform and international practice on TDF of non-personal data is not enough to affirm the existence of an international custom. Likewise, international jurisprudence has affirmed "the fact that the states declare their recognition of certain rules [the OECD Declara-

---

[191] *See infra* note 268 and accompanying text.

[192] Declaration, *supra* note 12, § a. The intention of the Declaration is to "*promote* access to data and information and related services, and avoid the creation of unjustified barriers to international exchange of data and information." *Id.* (emphasis in the original).

[193] The Export Administrations Act, 50 U.S.C. App. §§ 2401-2420 (1988). In the Dresser case, the export of technical data was denied under this Act. Kincannon, *supra* note 155; *see generally* Atwood, *The Export Administration Act and the Dresser Industries Case*, 15 L. & POL'Y INT'L BUS. 1157 (1983).

[194] This treaty's regime includes: a) "national treatment for business enterprises except where specified activities, notably communications, are included;" b) "most-favored nation treatment where national treatment does not apply;" c) "and general guarantees of 'fair and equitable' treatment." *See* Feldman and Garcia, *National Regulation of TDF*, 7 N.C. J. INT'L L. & COM. REG. 9 (1982); Horgan, *supra* note 41, at 364-67.

tion on TDF] is not sufficient to consider them as part of customary international law."[195]

b. Time Requirement

Neither the international doctrine nor the ICJ establishes a specific amount of years as a time requirement for the existence of an international custom. Traditionally, some scholars have affirmed that it was necessarily a uniform practice since time immemorial.[196] In contrast, others have sustained the possibility of an "instant custom" if the states consider themselves bound by such a rule.[197] The ICJ adopted an intermediate position on time requirements in the *North Sea Continental Shelf* case supporting the idea that at least a "short period" is necessary to affirm the existence of an international custom.[198]

Professor Jimenez Arechaga has pointed out that the time element required by the ICJ is only necessary to prove generality and uniformity of the custom invoked, rather than being a requirement by itself.[199] This statement is favorable for issues involving new technology of information. Because it is hard to consolidate into custom a particular practice regarding technology—due to the fast speed at which technology changes— one could consider the possibility of shortening the length of the practice requirement on issues

---

[195] Nicaraguan case, *supra* note 167.

[196] Juridiction of European commission of the Danube, 1926 P.C.I.J. (ser. C) No. 13, at 114 (Advisory opinion of Dec. 8, 1927) (Negulesco, J., dissenting).

[197] Cheng, *United Nations Resolutions on Outer Space: "Instant" International Customary Law?*, 5 INDIAN J. INT'L L. 23, 36 (1965). "[I]f states consider themselves bound by a given rule as a rule of international law, it is difficult to see why it should not be treated as such in so far as those States are concerned, especially when the rule does not infringe the right of third States not sharing the same *opinio juris*. . . . [T]here is no reason why an *opinio juris communis* may not grow up in a very short period of time among all or simply some [States] with the result that a new rule of international customary law comes into being among them." *Id.* at 37.

Other scholars, while not recognizing "instant" custom, as a general rule still do not require the repetition of acts by the states. A. D'AMATO, THE CONCEPT OF CUSTOM IN INTERNATIONAL LAW 91-98 (1971). Others have said that the mere adoption of international instruments such a guidelines or codes of conduct cannot be considered as "instant international law." Baade, *supra* note 58, at 13.

[198] The ICJ said:

> Although the passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law on the basis of what was originally a purely conventional rule, an indispensable requirement would be that within the period in question, short though it might be, State practice, including that of States whose interests are specially affected, should have been both extensive and virtually uniform in the sense of the provision invoked;—and should moreover have occured in such a way as to show a general recognition that a rule of law or legal obligation is involved.

North Sea Continental Shelf Cases (Den. v. W. Ger.), 1969 I.C.J. 4, 43 (Judgment of Feb. 20).

[199] Arechaga, *La costumbre como fuente del Derecho International*, 1 ESTUDIOS EN HOMENAJE AL PROFESOR MIAJA 392 (1979).

where new technology of information is involved.[200] For instance, it could be difficult to consolidate a practice on mechanisms for sending data across boundaries, but it would be easier to reach a practice on general aspects, such as free access to certain types of personal data, or the avoidance of creating unjustified barriers to the international exchange of data.

It is difficult to determine when the practice of TDF of personal data was consolidated. If one compares the practice of the 1970's with that of today, the increase is obvious. However, what is important is that today's analysis regarding national practice of TDF of personal data fulfills the objective element required by the ICJ for the existence of a custom.[201]

2. *Subjective Element: Opinio Juris*

To create a rule of customary law, the practice requirement must be accompanied by opinio juris. According to international jurisprudence, opinio juris has to be understood as "evidence of a belief that the practice is rendered obligatory by the existence of a rule requiring it."[202] The importance of opinio juris has been emphasized by some scholars and by the ICJ to the point of reducing the need to show general practice.[203]

a. Manifestation of Opinio Juris

The manifestation of opinio juris could be accomplished in different ways by sovereign states. For example, it could be expressed during diplomatic conferences, in the adoption of international organization resolutions, or by any other kind of public manifestation made by state representatives.[204] The questions then arise as to whether the COE Convention, the OECD Guidelines, and the OECD Declaration express an opinio juris; whether these instruments can be invoked as evidence of customary law; and whether these instruments crystallize customary law in the process of formation or whether they generate new customary law subsequent to its

---

200 Professor Gotlieb pointed out that the emerging of technology would modify the sources of international law because the relevance of the custom would be reduced due to the lack of the practice requirement. Gotlieb, *supra* note 33, at 128.

201 *See supra* note 167.

202 North Sea Continental Shelf Cases, *id.* Some scholars define opinio juris as a requirement "equivalent merely to the need for the practice in question to have been accompanied by either a sense of conforming with the law, or the view that the practice was potentially law, as suited to the needs of the international community." Thirlway, *supra* note 172, at 53-54.

203 Professor Schachter points out that a clearly demonstrated and strong opinio juris reduces the need to show general practice. *See* O. SCHACHTER, *supra* note 172, at 718. Although the ICJ did not deny the need of general practice in the Nicaraguan case, it did not provide its evidence throughout the judgment. *See* Nicaraguan Case, *supra* note 167.

204 *See* Diez de Velasco Vallejo, *supra* note 171, at 87.

adoption.[205]

COE Convention. In general, rules found in treaties can never be conclusive evidence of customary international law because the treaty reflects only the views of the parties participating in the elaboration of the instrument.[206] The ICJ, however, has sustained in the *North Sea Continental Shelf* case that it is possible that some rules adopted in treaties may become customary law.[207]

It is impossible to confirm that when the Convention was adopted there was a crystallized custom of TDF of personal data. However, the newness of the issue at the time suggests that the custom was still not formed.

As some scholars have mentioned, there is no particular rule that says whether a treaty is good evidence of opinio juris.[208] However, one can say that the COE Convention is not among those treaties adopted on a basis of reciprocal concessions, but rather on a mutual consensus which determined what rules were best to avoid the misuse and distortion of personal data when it was transferred across national boundaries.

It is this author's view that the Convention is evidence of opinio juris on a customary rule of TDF of personal data in a regional context. European States have often expressed, though governmental agencies at conferences and meetings, their intention to achieve a free flow of personal data when the recipient country has similar or equivalent data protection requirements. This implicitly expresses the idea of granting this rule higher rank than a conventional one. This is because the states believe that, unless all countries have similar requirements on TDF, individuals could be harmed by the distortion of information by a country lacking a data protection act.

Thus, the customary rule binds both those countries that have ratified and those countries that have only signed the convention. With respect to those European countries which were not parties to the convention, it is not clear whether they are bound by the customary rule.[209]

OECD Guidelines. The Guidelines probably cannot be considered

---

[205] These two possibilities were mentioned by the ICJ in the North Sea Continental Shelf Cases. *See supra* note 167.

[206] *See* Baxter, *Treaties and custom*, 129 RECUEIL DES COURS 25 (1970). Other scholars, like D'Amato, affirmed that treaties can be cited as authority for the existence of obligations in customary law. A. D'AMATO, *supra* note 197.

[207] Conventional or contractual rules in its origin is now accepted as opinio juris. "There is no doubt that this process is a perfectly possible one and does from time to time occur: it constitutes indeed one of the recognized methods by which new rules of customary international law can be formed." North Sea Continental Shelf Case, *supra* note 167. For further bibliography, see Marek, *supra* note 167.

[208] Professor Schachter affirms that such evidence is a question of fact and that they are "not pre-ordained nor are any particular answers foreclosed by rules of law." O. SCHACHTER, *supra* note 172, at 735.

[209] It has been argued that the extension of the custom is done in some cases, an

an instrument that manifests an opinio juris. Guidelines, in general, need to be broadly accepted to qualify as a source of international law. The limited and specialized membership in the OECD makes it unlikely that the OECD Guidelines could constitute customary international law.[210] In addition, guidelines generally do not prescribe legally enforceable rules, rather they formulate notions of law that are emerging in a specific field.[211]

The OECD Guidelines on TDF, in particular, formed part of a recommendation to the member states.[212] Even though some states have followed such recommendation,[213] it cannot be said that the Guidelines on TDF were an expression of opinio juris. Their provisions were not intended to be a governmental declaration of an opinio juris on TDF. Recommendations that the Council may make to member states have a non-binding nature, in contrast to decisions or declarations. However, if the TDF provisions were regarded as binding by a large number of states, then they could probably pass into the customary body of international law.[214]

OECD Declaration. The OECD Declaration on TDF is a multilateral instrument with different characteristics than those of the Guidelines. To a certain extent, the Declaration is a political instrument[215] because it is not mentioned as part of the decisional process in the Convention which creates the OECD. However, its importance is comparable to the Decisions of the Council, because once a Declaration is adopted by the specialized working group, it is then passed to the Council for its approval. Even though, in general, a Declaration expresses the willingness of the states on specific issues, it is not a unilateral declaration of states because the text is adopted in terms

---

attempt to impose the law to those states which are in a minority. Weil, *Towards Relative Normativity in International Law?*, 77 AM. J. INT'L L. 413, 438 (1983).

[210] Schwartz, *Are the OECD and UNCTAD Codes Legally Binding?* 11 INT'L LAW. 529, 536 (1977).

[211] *See supra* note 59.

[212] For the organization, structure and evolution of the OECD, see generally Guillaume, *L'Organisation de Coopération et de Développement Economiques et l'Evolution Récente de ses Moyens d'Action*, 25 ANNUAIRE FRANÇAIS DE DROIT INTERNATIONAL 75 (1979).

[213] Among the countries which have adopted the OECD Guidelines recommendations are: Australia, Japan, Finland and Canada. Other countries, such as New Zealand, have recognized the need to adhere to the recommendation. *See New Zealand: Privacy Bill Recommended*, TDR, June/July 1990, at 28.

[214] Davidow & Chiles, *The U.S. and the Issue of the Binding or Voluntary Nature of International Codes of Conduct Regarding Restrictive Business Practices*, 72 AM. J. INT'L L. 247, 255 (1978).

[215] Grewlich, *supra* note 13, at 14; K. SAUVANT, *supra* note 48, at 245. They sustain the possibility of becoming customary law with practice. Grewlich has called the Declaration a "living instrument" because, in his opinion, it will be enriched with the consultation and cases emerging from the different types of TDF that the Working Party on Information, Computer and Communication Policy has to study. Grewlich, *supra* note 13, at 14. Virally has sustained that political instruments, in general, provide *de lege ferenda* norms rather than *de lege lata*. *See* Virally, *A Propos de la "Lex Ferenda"*, 6 LE DROIT INTERNATIONAL: UNITÉ ET DIVERSITÉ 528 (1981).

that reflect the opinion of other states as well.[216]

In this author's view, the OECD Declaration on TDF of non-personal data is not a true political instrument. It manifests more than a simple concern with the technological developments in information and communication. However, it does not seem to reach the level of expressing an opinio juris on TDF of non-personal data.

The goals of balancing the free flow of information with the creation of unjustified barriers to the access of data, and reaching an international exchange of data—as it is expressed in the Declaration—qualify the custom on TDF of non-personal data as "status nascendi" exclusively.

C. General Principles of International Law and TDF

Although the general principles of law are considered to be a source of international law,[217] it is difficult to establish the content of these principles. There is no particular formula on how to define the general principles even though article 38 of the Statute of the International Court of Justice requires that they must be "recognized by civilized nations."[218]

In general, the principles of law apply to any of the issues relevant to the international community. TDF is an important issue to international relations. Therefore, there is no reason to exclude it from an application of the general principles of law.

Furthermore, it is not unusual that one particular situation is covered by different principles, or that some of those principles conflict with one another. In this case, it is necessary to find a balance between them in order to make them compatible. The analysis that follows on the relationship between TDF and the principle of freedom of information and state sovereignty serves as an illustration of this point. In addition, whether other general principles can be drawn from some of the existing international legal instruments on data protection addressed above, or from various systems of munici-

---

[216] Guillaume, *supra* note 212, at 86.

[217] "The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: [. . . .] c) the general principles of law recognized by civilized nations". Statute of the International Court of Justice, *supra* note 166, art. 38. However, other issues related to the general principles of law have been subjects of disagreement between scholars. The range of discussion varies from those who sustain that there is only a minor difference between the general principles of law and the custom (Reuter), to those who affirm that they are a subsidiary source of international law (Akehurst), to those who sustain that analogy is the technique to develop the general principles (Verdross), and to those who deny that the use of analogy is the appropriate means to construct the general principles (Rousseau). REUTER, DROIT INTERNATIONAL PUBLIC. SOURCES ET ACTES JURIDIQUES, 99 (1976); Akerhurst, *Equity and General Principles of Law* 25 INT'L & COMP. L.Q. 801, 817 (1976); C. ROUSSEAU, DROIT INTERNATIONAL PUBLIC 372 (1970).

[218] *Supra* note 166.

pal law is analyzed.[219] At this point, the discussion focuses on whether municipal law analogies may provide acceptable solutions to problems at the international level.

1. Freedom of Information and State Sovereignty Principles Related to TDF

a. Freedom of Information

The definition of TDF as the "transfer of data and/or information across national borders in machine-readable form and over telecommunication facilities"[220] seems to be connected with the principle of freedom of information. The important question, however, is whether the principle of freedom of information could be enforced by those who support the free flow doctrine in order to extend it to TDF of personal and non-personal data, or whether the principle of freedom of information can only be used within the framework in which it was conceived.

i. Formulation of the Principle

The principle of freedom of information is drawn from one of the most important human rights freedoms[221] adopted in many international instruments.[222] The content of the principle derives from Article 19 of the Universal Declaration of Human Rights and includes the "freedom to seek, receive and impart information . . . through any media and regardless of frontiers."[223]

The European Convention on Human Rights (ECHR) foresees

---

219 A comparative study would show whether certain principles exist in all or various systems of law. It is important that none of the legal systems are excluded. The existence of general principles in one legal system does not guarantee its generality. For example, the Court of Justice of the European Communities might apply general principles which are only common to the laws of the member states and not to the rest of the international community. Therefore, these principles could not be considered as general principles of international law in the sense established in article 38 of the Statute of the ICJ. *See supra* note 166.

220 *See supra* note 2, at 8 and accompanying text.

221 The General Assemby has characterized the freedom of information as "a fundamental human right and . . . the touchstone of all the freedoms to which the United Nations is consecrated." G.A. Res. 59, U.N. Doc. A/64, at 95 (1946). It would be very difficult to justify that in this context the General Assembly was including TDF in the notion of freedom of information.

222 The difficulty that nations have in establishing an international legal obligation to respect human rights has been noted by some scholars. The source of such obligations has been linked to the United Nations Charter. For a detailed explanation on the reasoning for deriving general principles from international rather than national sources, see Hevener, *General Principles of Law and the UN Covenant on Civil and Political Rights*, 27 INT'L & COMP. L.Q. 593, 603 (1978).

223 "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Universal Declaration of Human Rights, G.A. Res. 217, U.N. Doc. A/810, art. 19 (1948).

the same right,[224] although it does not include the right to "seek information."[225] The framers did not include this provision in order to avoid the possible discrepancies that could arise with the domestic constitutional provisions.[226]

The right to freedom of information was construed in a human rights framework but also as part of the right of expression and opinion.[227] The interpretation of the freedom of information clause may influence other issues such as TDF. The following examples illustrate this last point. The reference to "through any media"[228] might refer not only to traditional mass-communication but also to other more sophisticated telecommunication facilities. Moreover, it is possible that to "seek information through any media"[229] includes the most developed advances in communication, which have opened new frontiers to outer space, terrestrial, and undersea communication, as well as all of the problems that these issues involve.[230] In addition, it is not clear whether "regardless of frontiers" refers to frontiers within contracting states only, or whether it is a general statement that can be applied to any kind of frontiers.[231]

One should be especially cautious when applying the Freedom of Information clause to those questions that had not been addressed by the framers of the Universal Declaration at the time that the clause was drafted. First of all, it cannot be forgotten that the original meaning of the right to freedom of information was linked

---

224 "Everyone has the right to freedom of expression. This right shall include freedom to hold and to receive and impart information and ideas without interference by public authority and regardless of frontiers." European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, Europ.T.S. No. 5, art. 10, 213 U.N.T.S. 221 (1950).

225 *Supra* note 221.

226 The UDHR adopted that clause due to the strong influence of the American position to protect the "free flow" doctrine. The "free flow" doctrine appeared after World War II as a justification by the USA to keep the leading role in international politics. In this sense, the American strategy included substantial appropriation of the information and culture from other countries, strong cooperation with the private sector, and the establishment of new offices specialized in the treatment and transmission of information. *See* Y. EUDES, LA COLONIZATION DE LAS CONCIENCIAS: LOS CONTROLES USA DE EXPORTACION CULTURAL (1984). For a detailed development of the right of freedom of opinion and information, see Pinto, *La Liberte d'Information et d'Opinion et le Droit International*, 108 JOURNAL DE DROIT INTERNATIONAL 459 (1981).

227 *See supra* note 221 and *supra* note 222.

228 *Supra* note 221.

229 *Id.*

230 The advent of remote sensing satellites and direct satellite broadcasting has resulted in some problems regarding the attitude of various states towards freedom of information. *See* Poulantzas, *Direct Satellite Telecommunication: A Test for Human Rights Attitudes*, 28 REVUE HELLÉNIQUE DE DROIT INTERNATIONAL 226 (1975). In this sense, some states require a prior consent of the state to which the direct telecommunication is addressed. *Id.* at 226-27.

231 Some authors have said that the new communication technology has broken the geographic barriers and is moving towards a "world information grid." Marks, *International Conflict and the Free Flow of Information*, in CONTROL OF THE DIRECT BROADCAST SATELLITE: VALUES IN CONFLICT 65 (1974).

to freedom of opinion and expression. Thus, it included: a) freedom of the press—liberty to write about any person or thing, as well as to publish the writing without interference; and b) freedom of speech—including symbolic language or gesture.[232] Second, the problems involved in the advance of communication technologies belong to very different areas of study, such as remote sensing satellites and broadcast telecommunication and services, with their own legal framework. Third, it is important to have a human right that protects the freedom of information. However, this does not mean that TDF should have the same contents as this principal[233] should be used on TDF. Thus, there exists a link between TDF and the principle of freedom of information, but there is still some distance between them. TDF has developed and adopted other principles suitable to its own needs.

ii. Some Distance Between Freedom of Information and TDF

International doctrine is divided about the relationship between the principle of freedom of information and TDF. Some scholars have expressed their opposition to the application of the freedom of information principle to TDF.[234] Others have expressed the idea that TDF is a form of sending information, and that it should be protected by the principle to some extent.[235] Finally, other scholars assert that the concept of "information" has more than one meaning, and when the UDHR talks about "information," it only applies to one of the categories and not to the rest.[236]

It is true that TDF entails a special form of sending, storing, and processing information because of the different types of information

---

[232] Furthermore, the principle of freedom of expression and information has been broadly considered as an essential element to democracy; in this sense, it would be difficult to link TDF to democracy. Bullinger, *Freedom of Expression and Information: An Essential Element of Democracy*, 28 GERMAN Y.B. INT'L L. 88 (1985).

[233] The principle of Freedom of Information as established in the UDHR includes some limitations clauses based on "public order," "general welfare" and determined by "law" (article 29). *See supra* note 221. The ECHR includes some restrictions to the right to Freedom of Information as "prescribed by law" and "necessary in a democratic society" (article 10). *See supra* note 222; Holzberg, *The New World Information Order: a Legal Framework for Debate*, 14 CASE W. RES. J. INT'L L. 387, 390-95 (1982); Tajima, *Protection of Freedom of Expression by the European Convention*, 2 REVUE DE DROIT DE L'HOMME 658, 671 (1969).

[234] INTERGOVERNMENTAL BUREAU FOR INFORMATICS, FLUJOS DE DATOS TRANSFRONTERAS, PROTECCION DE DATOS Y DERECHO INTERNACIONAL, Doc. TDF 102 (May 1981) (Expressing some of the opposition).

[235] GARZON CLARIANA, INTERGOVERNMENTAL BUREAU FOR INFORMATICS, EL MARCO JURÍDICO DE LOS FLUJOS INTERNACIONALES DE DATOS, Doc. TDF 206 (1984).

[236] They contend that the first category is related to the protection of individual human rights; the second category emphasizes the state's responsibility for contracting the information through the frontiers; and the third category stresses the people's right to the information and to its development. Sur, *Vers un Nouvel Ordre Mundial de l'Information et de la Communication*, 27 ANNUAIRE FRANÇAIS DE DROIT INTERNATIONAL 35, 49-50 (1981).

that might be involved, because of its repercussion in the social, economic, and political life of a country, and because it requires sophisticated communication technology. Therefore, for several reasons it seems difficult to transplant the principle of freedom of information as stated in the UDHR or the ECHR to TDF. The first reason is that the existence of a general principle supporting the freedom of information does not imply a freedom of TDF. TDF reconciles the fundamental values of the respect for privacy and the freedom of information. Furthermore, as this Article has shown, the consensus within the OECD on TDF issues has always been difficult to achieve due to the fears of some state members of removing all the barriers on TDF and due to the positions held by governments. Nevertheless, a compromise was reached to avoid developing laws and practices in the name of the protection of individual liberties and privacy which would create additional barriers to TDF. Therefore, it is doubtful that the principle of freedom of information can be extended so easily to TDF.

The second reason is because the protection of the freedom of information was approached in the context of the protection of an individual freedom. Moreover, the limitation clauses to the freedom of information principle relate to the rights and freedoms of individuals, rather than to specific problems of TDF or other transfrontier activities.[237] Therefore, TDF would need to have its own limitation clauses and the international community would need to establish what justifications permit the creation of barriers on TDF. Thus, extending the limitation clauses of the freedom of information to TDF would be insufficient and unsuitable.

Finally, the problems raised by TDF have a very broad dimension that, by no means, can be solved by including them in the principle of freedom of information.

In this author's view, it is more appropriate to approach the principle of freedom of information as the first seed from which TDF grew than to say that both are interrelated. However, TDF has evolved independently, creating solutions for its own problems. TDF and the principle of freedom of information should not be considered the same issue; rather the interest in TDF in international relations is developing easily because of the existence of the principle of freedom of information that asserts the right "to seek, receive and impart information."

---

[237] Professor Damrosch addresses the issue of whether the right to receive information and express opinions would include transfrontier activities such as the raising of political campaign funds. Damrosch, *Politics Across Borders: Non-Intervention and Non-Forcible Influence over Domestic Affairs*, 83 AM. J. INT'L L. 11, 43 (1989).

b. Principle of Sovereignty of States

Once states realized the economic and political importance of having control over information,[238] they started to fear that losing control over that information would make them dependent on other states. Some scholars note that traditional views about sovereignty have changed toward a concern for "informational sovereignty."[239]

In any event, this principle of state sovereignty seems to be in conflict with the principle of freedom of information. On one hand, the principle of national sovereignty gives freedom to the states to establish rules regulating the flow of information. On the other hand, the principle of freedom of information is directly adverse to the setting of barriers to the transmission of information. It is obvious that a balance between both principles must be found to make them compatible for application to TDF.

As many international instruments recognize,[240] the state is sovereign to determine its own laws and to handle its internal matters as long as there is no interference with the interests of other states or with the accepted rules of international law. Therefore, states are free to decide their policy on data protection, as well as to set the requirements that data transferred to another country have to fulfill. Thus, the decision between promoting a protectionist policy[241] or a laissez faire policy on TDF belongs exclusively to the state.

Some developed nations consider the principle of sovereignty as an excuse given by developing countries to restrict the free flow of information, and thus they allege that the fundamental human right of freedom of information is denied. It may be true that restrictions on TDF could control cultural erosion and the vulnerability of the economy,[242] as developing countries claim. However, these restrictions can be an important barrier to achieving a higher degree of technological development. Foreign investment, mainly by multinational corporations, usually used to establish the basic technological network in developing countries could be reduced if strong restric-

---

238 Access to a flow of comprehensive and dependable "information is a key to political, economic, social and cultural developments." Chen, *Human Rights and the Free Flow of Information*, 4 N.Y.L. SCH. J. INT'L L. AND COMP. L. 39 (1982); *see* Bortnick, *International Information Flow: The Developing World Perspective*, 14 CORNELL INT'L L.J. 333 (1981).

Developing countries have not been the only ones to express their concern for sovereignty issues; so have developed countries such as Canada and Sweden. *See supra* note 32, at 255.

239 Gotlieb, Dalfen and Katz, *supra* note 32 at 254-55.

240 U.N. CHARTER art. 2.

241 For example, Brazil is one of the countries with protectionist legislation protecting TDF. Brazil requires that multinational corporations develop local subsidiaries, personnel and facilities to carry out the process of data within the developing nation. Bortnick *supra* note 238, at 340-42. *See generally* Study on TDF and Brazil, *supra* note 189.

242 For a detailed study on these issues, see Note, *Freedom of Information versus National Sovereignty: The Need for a New Global Forum for the Resolution of Transborder Data Flow Problems*, 10 FORDHAM INT'L L.J. 263 (1986-87).

tions on TDF are enacted.[243]

In an international forum the need to balance the principle of freedom of information and state sovereignty has been suggested by some scholars[244] and has been discussed in an international forum. The rules proposed set forth the following points: a) the limits established by the states that affect the transfer of information have to be justified and internationally accepted; b) the actions carried out by the states must be in good faith; c) the limits established by the states cannot be discriminatory on the basis of an individual's sex, race, or other social conditions, nor on the basis of international economic relations.[245]

Although some of the limits expressed in the previous proposal were accepted internationally before TDF arose—such as the good faith requirement[246]—in this Author's view, it is significant that they were framed within the TDF context. This proposal when adopted was the first international instrument that combines some of the broadly accepted policies and principles of international law[247] in relation to TDF. The relevance of this proposal has been reduced since the organization that adopted it was dissolved (IBI). However, it would be very convenient if another international organization, such as the United Nations,[248] would undertake this type of work on the regulation of TDF and other related issues.

2. *TDF and Other General Principles of Law*

Besides the possibility of applying traditionally accepted principles of law, it is also important to address whether there are other types of general principles that might apply more specifically to TDF. Because all the principles of law need not belong to the same category,[249] it is possible to find a principle that would apply to a particu-

---

[243] Sauge & Edwards, *Transborder Data Flows: The European Convention and United Kingdom Legislation*, 35 INT'L & COMP. L.Q. 710, 713 (1986). *See generally* Glasner, *Multinational Corporations and National Sovereignty* in TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS 335 (1986); Coombe & Kirk, *Privacy Protection and TDF: A Corporate Response to International Expectations*, BUS. LAW., Nov. 1983, at 33; Dunn, *Advice to the U.S. Corporation Operating Abroad: The Costs of Transporting Information*, 9 ASILS INT'L L.J. 61 (1985); Samiee, *Transnational Data Flow Constraints: A New Challenge for Multinational Corporations*, 18 J. INT'L BUS. STUD. 141 (1984).

[244] Garzon Clariana, *supra* note 235.

[245] Intergovernmental Bureau for Informatics, *Flujos de Datos Transfronteras, Proteccion de Datos y Derecho International*, Doc. TDF 102, at 15 (1981). Clariana, *supra* note 235, at 16.

[246] Goodfaith is a general limit according to the UN Charter and the DECLORATION ON PRINCIPLES OF INTERNATIONAL LAW CONCERNING FRIENDLY RELATIONS AMONG STATES IN ACCORDANCE WITH THE CHARTER OF THE UNITED NATIONS. G.A. Res. 2625 (1970).

[247] For a discussion on policies and principles in international law, see O. SCHACHTER, *infra* note 249, chap. 2.

[248] It is my hope that after the first steps taken by the UN it will continue the work on TDF. *See supra* note 23 and accompanying text.

[249] Different categories of GPIL include: Principles of municipal law recognized by civilized nations; General principles of law derived from the specific nature of the interna-

lar area of international relations such as TDF. Moreover, the growth of international relations and the development of different legal cultures and traditions that will enrich international law would also pave the way for the general principles of law to become an important instrument for achieving further development in new areas of international law.[250] Thus, the general principles of law must be analyzed in further detail.

An initial search for principles of law related to TDF has already been made by the Scandinavian scholars. Their concern about the lack of international regulation of TDF motivated them to elaborate a study to determine what general principles could be drawn from a number of treaties and conventions[251] that did "not have a direct link with telecommunication law" but that might be applicable to TDF.[252]

The focus of this Article differs from that of the Scandinavian scholars. This Article's analysis is based on the provisions adopted in the national and international instruments on data protection. Because the ruling of these instruments on TDF deals exclusively with personal data, it will be almost impossible to include a discussion of TDF of non-personal data, although, in this author's opinion, the latter would need a specific analysis.

---

tional community; Principles intrinsic to the idea of law and basic to all legal systems; Principles valid through all kinds of societies in relationships of hierarchy and coordination; Principles of justice founded on the very nature of man as a rational and social being.*See* O. SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE: GENERAL COURSE IN PUBLIC INTERNATIONAL LAW (1985). Even though each category is analytically distinct, it is not unusual for a principle to fall into more than one category. *Id.* at 75.

In addition,"[i]t is outside the Court's jurisprudence where we must look for the most meaningful contribution of the 'general law' to the development of international law. Most of the new international economic law . . . has for the greatest part developed outside the sphere of the International Court of Justice." Friedmann, *General Course in Public International Law*, 127 RECUEIL DES COURS 41, 149 (1969).

250 Diez de Velasco, *supra* note 171, at 97.

251 *See* J. BING, P. FORSBERG & E. NYGAARD, LEGAL PROBLEMS RELATED TO TRANSBORDER DATA FLOWS 59 (OECD Series of Information Computer Communication Policy No. 8, 1983). In particular, the Conventions examined are: the Convention on International Civil Aviation; the Convention and Statute on the International Regime of Railways; the Barcelona Convention and Statute on Freedom of Transit; International Telecommunication Convention; Universal Postal Convention; and Universal Copyright Convention. *Id.* Concerning the lack of data protection, see generally Sieghart, *The Protection of Personal Data—Lacuna and Overlap*, in TRANSNATIONAL DATA FLOW AND THE PROTECTION OF PRIVACY 244 (OECD Series of Information Computer Communication Policy No. 1, 1979).

252 The Spanish doctrine has been severely critical about the Scandinavian argument. Their critique is related, in particular, to the method used to determine the general principles of international law. In this sense, Professor Garzon Clariana asserts that the analogical method used is only appropriate to determine *arguments of policy*, but not to determine international law. Garzon Clariana, *supra* note 235. For a more recent criticism made in similar terms, see Piñol Rull, *supra* note 158, at 147.

a. Search for a General Principle Linked to TDF

Some scholars have described the principles[253] mentioned in the OECD Guidelines and in the COE Convention as the "hard core" of the general principles put forward by these organizations and embraced in some national legislation.[254] Questions arise as to whether these basic norms could be classified as general principles of law and whether they are recognized by civilized nations.

Although it seems difficult to attribute the category of general principles of law to these very specific, basic rules, a new formulation enhancing the basic rules mentioned in those international instruments would qualify as a general principle of law. This new formulation would have a broad application and a high degree of abstraction.

Thus, it is important to find the underlying common ground between the TDF's basic rules provided in the COE Convention and the OECD Guidelines and the existing municipal laws. The general purpose of those international instruments is to safeguard personal rights when personal data is automatically processed. Such aim is achieved by imposing double standards.

The first requirement is imposed on the data transferred abroad. There are a variety of limitations on data, such as quality, a collection limitation, specification of purpose, a use and disclosure limitation, security safeguards, the openness principle, a time limitation, and accountability and social justification norms.[255]

The second standard is imposed with respect to the recipient of the data transferred. The recipient is under a duty to grant the data subject access to the data relating to him, to update and correct any of the wrongfully stored data, and to take the necessary precautions to prevent the misuse of data and access by third parties.

It is clear that a formulation of a general principle of international law regarding TDF must be consistent with these two sets of requirements that are common to international instruments and existing municipal laws. A possible formula for the adoption of a new principle of international law related to TDF would be that TDF of personal data cannot be done arbitrarily, and minimum standards of

---

[253] It is important to clarify that when the COE Convention, the OECD Guidelines or some national laws mention TDF principles, they do not refer to them as general principles of law, but rather as basic rules of TDF.

[254] Justice Michael D. Kirby uses a dual expression to categorize those principles: basic rules and general principles. While describing the proliferation of privacy laws at the beginning of his article, Kirby refers to the " 'basic rules' which can be used as a benchmark for privacy" protection. Kirby, *supra* note 80, at 27. In a latter stage of his article, he affirms that the "identification of *general principles*" by international bodies and the legislation of some countries will help the rest of the countries which are in the process of developing such laws. *Id.* at 29-30 (emphasis in original).

[255] For a more detailed explanation of these principles, see *supra* notes 82, 107 and accompanying text.

quality (such as those mentioned in both the Convention and Guidelines) and certain guarantees to the data subject must be achieved. The emergence of new principles of international law proves that they are not "framed in a stable category," and instead they evolve and reflect the complexity of international relations.[256]

The question arises whether analogy has been used to determine the above principle of law on TDF. It is widely accepted by international legal scholars that analogy can not be a source of international law.[257] In the *South-West Africa* case[258], the ICJ denied the validity of analogies drawn from municipal law because the analogies were false and irrelevant.[259] In a separate opinion, Judge Sir Arnold McNair states that the duty of the international tribunals when confronted with a new legal institution is not to import the rules from private law, but rather to look for the policy and principles of those institutions and to adopt them according to the needs of international law.[260]

This Author agrees with the dissenting opinion of Judge McNair, although believes that the problem posed by TDF has a substantially different dimension than the one discussed in the *South-West Africa* case, because the notions involved in TDF not only have been discussed in international fora, but also have been adopted in international instruments. Nevertheless, if the adoption of municipal law principles were appropriate to be applied on an international level,[261] and they were recognized by civilized nations, then, in this Author's opinion, they should be adopted.

b. The Acceptance of a General Principle on TDF by "Civilized Nations."

In order for the above principle on TDF to be a feasible one, the terms under which it is formulated must be "recognized by civilized nations." Although it is always difficult to determine the number of

---

256 O.SCHACHTER, *supra* note 249.

257 "Analogy is not a source of right." Rousseau, *supra* note 217, at 372. Other scholars discuss the need to use analogy in order to obtain general principles, a fact which places the general principles in a lower level as a subsidiary source. According to Akehurst, "[t]he fact that general principles of law can usually be applied only by way of analogy, and only in appropriate circumstances, may seem to limit their utility . . . they are a subsidiary source of international law, overshadowed by treaties and custom." Akehurst, *supra* note 217, at 817.

258 International Status of South-West Africa, 1950 I.C.J. 128, 132 (Advisory Opinion of July 11).

259 The I.C.J. has described a mandate's nature. "The object of the Mandate regulated by international rules far exceeded that of contractual relations regulated by national law. . . . It is not possible to draw any conclusion by analogy from the notions of mandate in national law or from any other legal conception of that law." *Id.*

260 *Id.* at 148 (McNair, J., concurring).

261 "[M]unicipal law analogies may provide acceptable solutions for the states concerned or for a tribunal empowered to settle a dispute." O. SCHACHTER, *supra* note 249.

countries, and which countries, fulfill the "civilized" requirement of article 38(c), it is generally accepted that OECD's state members constitute a good representation of civilized nations. However, it is also true that not all its members have enacted domestic laws after the adoption of the Guidelines on TDF. Then it must be examined whether this would impair the existence of the principle, and whether the UN Guidelines would fulfill the requirement of good representation of civilized nations. The purpose underlying the Guidelines is to state a minimum guarantee with respect to computerized personal data files kept within the state or transferred abroad. Thus, this aim is in accordance with the terms used above in the formulation of a new general principle related to TDF.

Many scholars have stated that the only reliable way to prove whether a general principle is recognized by civilized nations is by examining the laws of different countries.[262] Thus, it is necessary to carry out a comparative study of the different legal systems.

The following is the result of an examination of the family groups of legal systems:

a) In most English speaking countries, or common law countries, the principle on TDF, as stated above, is well established in the overall provisions on data protection.[263]

b) Many civil law countries, particularly the European countries, include the above principle throughout their domestic laws.[264] With regard to the countries of South and Central America that follow the

---

[262] Akehurst, *supra* note 217, at 818; Hevener, *supra* note 222.

[263] This is the case in Australia, Canada, and The United Kingdom. *See supra* note 79. New Zealand has an Official Information Act in which some of the principles of the OECD Guidelines are already adopted and it is about to pass a bill setting up a data protection authority which applies the OECD principles on data protection. *See supra* note 213.

The United States' Privacy Act of 1974 develops the same principle which was based on the Privacy Protection Study Commission Report. The Report states:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data and must take reasonable precautions to prevent misuse of the data.

REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 501 (1977).

Hong Kong passed "Data Protection Principles and Guidelines" in 1989. *Hong Kong: Privacy Law Drafting Committee Formed*, TDR, Feb. 1990, at 25. Although these guidelines are not legally binding, they are being used until a law on data protection is prepared and passed. *Id.*

[264] For the European data protection acts, see *supra* note 56. Japan has also passed a data protection law. Hiramatsu, *Japan Adopts Privacy Protection Act*, TDR, Feb. 1989, at 22. The existing Japanese data protection covers the public-sector exclusively. Hiramatsu, *Ja-*

civil law tradition, no data protection acts have been adopted yet. However, some governments are working on the elaboration of drafts that will reflect the same principles as those adopted in the OECD Guidelines and in the other European Acts.[265] In addition, in the "Second World Conference on TDF Policies"[266] the Latin American countries' representatives agreed on the need to carry out a thorough study on the general principles applied to TDF.[267]

c) Some communist or socialist countries are passing legislation on data protection that includes the basic norms set out in the OECD Guidelines and COE Convention.[268] Other communist and socialist countries have expressed the need for data protection acts and the willingness to undertake such an enterprise.[269]

d) Although there are no data protection acts enacted within the African countries, they are conducting studies on common statements on TDF and principles that should be adopted.[270] Some recommendations have been adopted during regional conferences on African Information Integration. These recommendations support the establishment of regulation to protect data against misuse.[271]

---

pan's Private-Sector Data Protection, TDR, May 1990, at 11, 12. However, there is a movement to include the private-sector under the same principles. *Id.* at 12.

265 Colombia, Brazil and Argentina are some examples. *See Argentina Needs Privacy, TDF Laws*, 8 TDR 381 (1985).

266 *See* Pipe, *Report on the Conference*, 7 TDR 253 (1984). The Second World Conference on Transborder Data Flow Policies, organized by IBI, was held in Rome in 1984. *Id.*

267 SECOND WORLD CONFERENCE ON TRANSBORDER DATA FLOW POLICIES, FINAL STATEMENT (June 26-29, 1984), *reprinted in* Pipe, *Report on the Conference*, 7 TDR 253, 282 (1984).

268 Some examples are: Slovenia, one of the federal republics of Yugoslavia, has adopted a Data Protection Act on March 7, 1990. Cebuli, *Yugoslavia: Slovenia Recognizes Data Protection Rights*, TDR, May 1990, at 26-27. Hungary is in the process of passing a bill on "principles of the Data Protection Act." Sólyom, *Hungary: New Data Protection Rights*, TDR, Nov. 1989, at 29, 32.

269 This is how it was expressed during the International Data protection Seminar held in Budapest on April 24-28, 1990, where participants of Hungary, Bulgaria, Czechoslovakia, Poland, the German Democratic Republic, Romania, the Soviet Union, and Yugoslavia participated. *See* Schindel, *Budapest Seminar: Emerging Data Protection in Eastern Europe*, TDR, June/July 1990, at 6-7. Some scholars have analyzed the increase of TDF and the need to develop infrastructural ties on TDF between East and West. *See* Monkiewicz, *Transborder Data Flows in East-West Relations*, in EUROPE SPEAKS TO EUROPE 72 (1989).

270 In a conference held by the Heads of State and Governments of the African countries, the main concern was to adopt a program on informatics which would be suitable to their needs. *See Declaration of Yamoussokro: Conference on Informatics and Sovereignty, a Contribution to the Lagos Plan of Action*, TDR, May 1985, at 252-53. In addition, undertaking a study on the dispositions adopted by international organizations in relation to TDF was considered. *Id.*

According to the comments on the result of that Conference, the need to adopt the basic principles of TDF at an international forum was discussed. *See* Allotey, *Guidelines to Data Protection Law in Africa*, TDR, June 1985, at 313; Allotey, *supra* note 35, at 40.

At the 2nd World Conference on TDF, similar statements and ideas were expressed by the representatives of the African countries. *See supra* note 266.

271 See recommendation number five abopted at the Conference on African Informatics Integration, reprinted in U.N. Doc. ST/CTC/23 Annex IV (1980).

Therefore, it could be assumed that these countries recognize the existence of a general principle on TDF.

It is clear that most countries with a Western tradition have already adopted in their domestic law such a principle of TDF. Among the countries with a non-Western tradition, some have expressed this principle in their municipal laws. Others are progressively adopting it in similar terms. Thus, not just a minority of states, but a variety of states representing different families of legal systems have adopted a set of basic rules establishing minimum standards on personal data sent abroad. This emphasizes the idea that the transfer of personal data cannot be made arbitrarily, and that the individual affected should be protected against the misuse and distortion of their personal data. In addition to domestic law, the international instruments on TDF, particularly the UN Guidelines, show that it is not just a western principle, but it is accepted by the international community in general.

IV. Conclusion

This Article has examined what role the traditional sources of public international law have played in regard to TDF. At the time it became technically possible and feasible to transfer data across borders, it was impossible to predict in which manner and to what extent such transborder data flow would be regulated internationally twenty years later. Today, TDF has been regulated extensively.

The majority of international instruments regulating TDF focus on the transmission of personal data. The most important instruments—the OECD Guidelines and the COE Convention—are very similar in their approach and provisions promulgated therein. This is striking since the interests pursued by these two international organizations are different. The objective pursued by the OECD Guidelines has been achieved. The OECD Guidelines have served as a guide to many countries in the preparation and enactment of their domestic acts on data protection. The adoption of the COE Convention by most European countries has encouraged the European uniformity on TDF concerning personal data.

The UN Guidelines take the same approach as one of the two above-mentioned instruments. Since the UN Guidelines have been approved by the General Assembly, they reflect the consensus of the international community on the legal aspects of the cross-border flow of personal data.

As far as the transborder flow of non-personal data is concerned, the international instrument adopted—the OECD Declaration—is merely a first step in its regulation. The resistance of the business community against establishing any restrictions on the transfer of data that could impair the free flow of information, and

affect economic intrests leads to the conclusion that it will take a considerable period of time before the regulation of TDF of non-personal data reaches the same level as the regulation of TDF of personal data.

As to any international custom of TDF concerning personal data, if any custom exists, it is a regional one. A regional custom, consisting of general restrictions on the free flow of personal data from one country to another country unless similar or equivalent protection exists in the recipient country, has been established in the European continent. The state practice is evidenced by the national laws adopted on this subject, by the activities conducted, and by the decisions rendered by the national data commissioners and domestic courts. It is difficult to say when this practice reached the level of custom. However, based on this Article's analysis of the state practice, it is concluded that the objective element required by the ICJ for the existence of a custom has been met. With respect to the evidence of the subjective element, or opinio juris, on TDF concerning personal data can be found in the COE Convention. This is especially true because the Convention was not comprised of the states, rather it was an instrument in which the European countries evidenced their consensus on this subject. Moreover, the customary rule has been expressed by the data commissioners in similar terms outside the COE framework.

Why this custom arose exclusively within the European context might be explained by cultural historical reasons. Today, the Eastern European countries have shown interest in joining the Western European tradition on TDF. The scope of regional custom on TDF concerning personal data may be enlarged as soon as the Eastern European states accede to the COE Convention and develop some state practice.

The OECD Guidelines do not constitute evidence of opinio juris on a customary rule of TDF. The provisions of these instruments were not intended to be an expression by the states of an opinio juris of TDF; rather they were adopted as recommendations to the member states on how to approach the regulations of TDF concerning personal data. Based on this Article's analysis of a possible customary norm of TDF concerning non-personal data, such norm is in "status nascendi" at the most. State practice has not been developed sufficiently to consider the OECD Declaration as a manifestation of opinio juris on this point is questionable.

Finally, based on this Article's examination of the general principles of international law, it can be concluded that the principle of freedom of information, one of the most important principles within the human rights context is related to TDF. However, TDF is nothing more than one species of the genus of the freedom of informa-

tion. TDF has developed a set of specific problems different than those involving the principle of freedom of information. These problems cannot be solved by merely applying the answers that resolve general questions concerning the freedom of information. Therefore, a specific legal regime regulating TDF is needed.

Some states have used the principle of sovereignty to justify the restrictions they have imposed on the free flow of information. The principle of sovereignty of states and the freedom of information are by nature incompatible. Except for the IBI, no international organization has analyzed how these two competing principles should be reconciled within the context of TDF.

The search for a general principle regarding TDF that is recognized by all—or almost all—civilized nations leads to a comparative study concerning the different legal systems. All the family groups of the legal systems agreed upon the principle that personal data cannot be transferred across the borders arbitrarily, thus creating both minimum standards on the quality of the data transmitted and certain guarantees for the person to whom these data relate.

In short, this Article has described how the regulatory vacuum created by the rapid development of computer technology in the 1970's has slowly been filled by regulatory instruments of different natures. As far as personal data are concerned, a regional rule of customary law has been established. It is this Author's hope that since the UN Guidelines have been approved by the General Assembly, the UN will take additional steps to achieve international regulation on TDF of personal data.